6ª ed

(in)Segurança na Prescrição Eletrónica

Uma análise do atual sistema e proposta de um sistema de prescrição eletrónica

Hugo André Malheiro Rodrigues

MESTRADO EM
INFORMÁTICA MÉDICA
2º CICLO DE ESTUDOS

Fev|2013

6ª ed

(in)Segurança na Prescrição Eletrónica

Uma análise do atual sistema e proposta de um sistema de prescrição eletrónica

Hugo André Malheiro Rodrigues

MESTRADO EM
INFORMÁTICA MÉDICA
2º CICLO DE ESTUDOS

Digitally signed by HUGO ANDRÉ MALHEIRO RODRIGUES
Date: 2013.05.28 05:03:11 +01'00'
Adobe Acrobat version: 11.0.0

ORIENTADORES
Prof. Doutor Manuel Correia, professor auxiliar da FCUP
Prof. Doutor Luís Antunes, professor associado da FCUP

Fev|2013

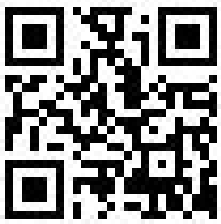
Agradecimentos

Aos meus professores, Doutor Manuel Eduardo Correia e Doutor Luís Antunes, pelo apoio incondicional, incentivo permanente e pela forma como se disponibilizaram para me guiarem e orientarem neste percurso académico conducente ao grau de mestre, registo e anuncio o profissionalismo.

À Joana, pela paciência, pelo apoio incondicional, pelas inúmeras horas de trabalho a meu lado, pelo incentivo férreo e pela motivação que sempre se dignou emprestar nos momentos de trabalho intenso e de desalento.

A todos os que, direta ou indiretamente, contribuíram para a construção deste trabalho, não elencados mas registados nas nossas memórias.

Por fim, mas não em último lugar, aos meus pais e ao Jorge, pelo apoio emocional e afectivo que me deram ao longo desta caminhada, em permanente contacto e preocupação.



Resumo

Introdução: A introdução do sistema de prescrição eletrónica (SPE) em 2004 produziu uma importante evolução no sistema de saúde português que permitiu uma "semi-desmaterialização" e melhor controlo das prescrições realizadas. Anteriormente, as prescrições medicamentosas limitavam-se a receitas escritas à mão cuja leitura era por vezes complexa e cuja potencialidade de fraude se tornou cada vez maior. Com o evoluir dos cuidados de saúde primários e da medicina preventiva, o número de prescrições aumentou exponencialmente, o que tornou a certificação das mesmas numa tarefa complicada e consumidora de recursos. Desde então têm sido criadas legislações orientadas a que esse sistema se tornasse o principal meio de prescrição, tendo sido alargado às instituições de saúde privadas o acesso e a obrigatoriedade de uso do SPE.

Problema: O SPE, enquanto recurso do sistema nacional de saúde, revelou-se uma mais-valia quer pela adesão médica, quer pela possibilidade de gestão e controlo das prescrições. A partir de 2011 decretou-se a obrigatoriedade do uso SPE, implementado em Portugal nas instituições privadas por meio de empresas de *software* de prescrição que disponibilizam os recursos tecnológicos necessários para o transporte dos dados de prescrição até ao Ministério da Saúde. A introdução de terceiras entidade no circuito das prescrições eletrónicas, fragiliza os níveis de segurança na prescrição e compromete a confidencialidade e privacidade dos dados pessoais dos médicos e dos seus utentes.

Objectivos: Este trabalho tem como objectivos: descrever o atual sistema de prescrição e identificar falhas de segurança que podem colocar em causa a privacidade dos dados das prescrições e potenciam a fraude; descrever os principais SPE existentes na Europa; propor medidas passíveis de serem implementadas no atual SPE de forma a permitir uma melhor proteção dos dados das prescrições eletrónicas, capazes de certificar os prescritores e de manter a integridade e segurança dos dados pessoais dos médicos e dos seus utentes.

Métodos: A descrição do atual sistema de prescrição foi produzida com base nas informações fornecidas por pessoal médico e pelo Ministério da Saúde. Para o efeito recorreu-se à realização de um inquérito orientado para os responsáveis pelos sistemas de prescrição nas instituições privadas. A elaboração de propostas de melhorias ao sistema de prescrição atual é realizada tendo por base os conceitos e as melhores práticas de segurança atualmente disponíveis, tendo sempre em linha de conta a viabilidade da sua inclusão e implementação no SPE atualmente existente e em produção.

Abstract

Introduction: The deployment of the SPE (Electronic Prescription System) constituted an important evolutionary step for the Portuguese Health system, as it promoted the dematerialization and better control of the emitted prescriptions. Before the SPE, medical prescriptions were handwritten and where thus very difficult to read and potentially very vulnerable to fraud. The last decades massive evolution of medical knowledge, the generalization of preventive medicine practices and new drugs developed by the pharmaceutical industry have led to an exponentially increase in the number of prescriptions, whose verification and certification has thus become a very hard and expensive task for the health service. The Electronic Prescription System (EPS) is a National Health Service (NHS) resource that has proved time and again to be an invaluable asset, not only by its high level of healthcare professionals acceptance and adherence, but also by the provided increased level of management and control with the associated reductions in prescription costs and levels of fraud.

Problem: Since 2011, in Portugal it is mandatory to prescribe through an electronic system. The NHS institutions may use the Internal Health Network (RIS-"Rede Interna da Saúde") to transmit electronic prescriptions. Because private institutions are not allowed to connect with RIS, the health ministry negotiated with approved software companies to provide prescription software/interfaces and act as gateways to relay prescription data from the private practitioners to the Health Ministry information systems.

We contend the use of those companies in this circuit weakens the security level of the national EPS and can severely compromise the doctors' trust in the system and the patients' privacy.

Aim: Our main aim is to extend the current EPS model to protect prescription integrity, increase its level of confidentiality and to strongly authenticate its main actors and provide the EPS with strong non-repudiation properties.

To better understand and achieve these objectives, we start by describing in detail the current Portuguese prescription system in order to better identify security vulnerabilities that may compromise personal sensitive data and potentiate fraud. We will also provide a comparison survey of the main European prescription systems to better understand how they have dealt with similar problems and use this knowledge and experience to improve upon the Portuguese EPS.

Methods: The description of the actual prescription system has been based on information provided by medical practitioners, legislation and normative documents published by the Health Ministry. We have also employed one questionnaire to determine the perceived security doctors have about of the actual prescription systems and another to better categorize other countries prescribing systems. Our proposal is based in current best of breed security protocols and best security practices, conductive of practical and pragmatic implementations.

Expected Results: During the course of this work we have identified several security problems and privacy issues related with the current PEM model. They comprise excessive personal information demanded from the medical professionals by the services companies, weak authentication procedures, weak integrity and validity mechanisms, easily replicable prescriptions, non-real-time validation of prescription data, potential misuse of patients' information by software companies and lack of confidentiality during the dispensation process at the pharmacies. These are some of the problems we want to tackle with the proposed model described by this document.

Índice

Agradecimentos ..... **i**

Resumo ..... **ii**

Abstract ..... **iv**

Índice ..... **vi**

Acrónimos ..... **viii**

Índice de Figuras ..... **ix**

Índice de tabelas ..... **x**

Prefácio ..... **xi**

1 Introdução **1**

1.1 Breve história do SNS 2

1.2 Contexto Atual 6

1.3 Material e Métodos 11

1.4 Trabalhos Realizados 14

2 Estado de Arte **16**

2.1 Privacidade, Confidencialidade e Segurança 16

2.2 Segurança Eletrónica 18

2.2.1 Chaves Simétricas e Chaves Assimétricas 20

2.2.2 Método DES e AES 24

2.2.3 Algoritmo RSA 27

2.2.4 Assinaturas 31

2.2.5 Assinaturas de Grupo 35

2.3 Infraestrutura de Chaves Públicas 37

2.4 Smartcards 41

2.4.1 Cartão de Cidadão 45

2.4.2 Cartão da ordem dos médicos 51
2.5 Prescrição Eletrónica de Medicamentos 54
2.5.1 Publicações sobre a Segurança na PEM 57
2.5.2 Prescrição Eletrónica na Europa 61
2.5.3 Projeto epSOS 66
3 Sistema de Prescrição Atual 69
3.1 SPM - Sistema de Prescrição Manual 70
3.2 SPE - Sistema de Prescrição Eletrónica 74
4 Avaliação da Percepção dos Riscos de Segurança na PEM 83
4.1 Introdução 83
4.2 Métodos 84
4.3 Caraterização da Amostra 85
4.4 Resultados 86
4.5 Discussão dos Resultados 89
4.6 Conclusão 94
5 SPE Proposto – Modelo eletrónico 95
6 SPE Proposto - Modelo físico 101
6.1 QR-Code da Receita (QR-Presc) 104
6.2 QR-Code do Certificado (QR-Cert) 109
7 Conclusões 113
8 Trabalho Futuro 118
9 Anexos 119
9.1 Anexo 1: Questionário de Avaliação da Percepção dos Riscos de Segurança nos Profissionais de Saúde 120
10 Referências 123

Acrónimos

ACSS – Entidades Público-Privadas
AES – Advanced Encryption Standard
ARS – Administrações Regionais de Saúde
CA – Certification Authority
CCF – Centro de Conferência de Facturas
CPE – Cartão profissional eletrónico
DES – Data Encrypt Standard
DSA – Digital Signature Algorithm
DSS – Digital Signature Standard
EPE – Entidades Público-Privadas
ERS – Entidade Reguladora da Saúde
EEPROM – Electrically Erasable Programmable Read-Only Memory
epSOS– Smart Open Services for European Patients
MAC – Message authentication code
PEM – Prescrição Eletrónica de Medicamentos
PDS – Plataforma de Dados de Saúde
PGP – Pretty Good Privacy
PKI – Public-Key Infrastructure
RCU2 – Resumo Clínico Único do Utente
RIS – Rede de Informação da Saúde
RSA – Modelo Criptográfico Assimétrico do Rivest, Shamir e Adleman
SMS – Serviços Médico-Sociais
SNS – Serviço Nacional de Saúde
SOA – Service-Oriented Architecture
SPE – Sistema de Prescrição Eletrónica
SPM – Sistema de Prescrição Manual
SPMS – Serviços Partilhados do Ministério da Saúde
TTP – Trusted third party

Índice de Figuras

Figura 1: Exemplo de formulário de inscrição numa empresa de software 7
Figura 2: Métodos de Seleção de Artigos 12
Figura 3: Exemplo de chave simétrica 20
Figura 4: Exemplo de encriptação com uma chave Assimétrica 21
Figura 5: Exemplo de autenticação com uma chave Assimétrica 22
Figura 6: Processos de Encriptação e desencriptação com o algoritmos DES 24
Figura 7: Esquema de funcionamento do DES (CBC, CFB, OBF) [29] 25
Figura 8: Exemplo dos componentes necessários para gerar uma chave RSA 29
Figura 9: Assinatura da *hash* de um documento 33
Figura 10: Exemplo de criação de uma chave de grupo 35
Figura 11: Representação de uma PKI (*Public Key Infrastructure)* 39
Figura 12: Exemplo de um smartcard, o chip interno e dos seus conectores 43
Figura 13: Cartão de Cidadão (frente e verso) 46
Figura 14: Informação contida no Cartão de cidadão 48
Figura 15: Esquema de certificação usado no cartão de cidadão 50
Figura 16: Esquema de um SPE 55
Figura 17: Esquema representativo do *TROPPI-project* [58] 59
Figura 18: epSOS - Lista de países aderentes ao projeto 66
Figura 19: epSOS - Projeto-piloto de prescrição e de dispensa eletrónica 67
Figura 20: Receita Manual (2012) 70
Figura 21: Receitas Manuais (2013) 70
Figura 22: Exemplo das Vinhetas em vigor a partir de 2013 (Pantone 305 U) 71
Figura 23: Esquema do Atual Sistema de Prescrição Manual 72
Figura 24: Esquema do Atual Sistema de Prescrição Eletrónica 75
Figura 25: SPE, seus intervenientes e o potencial fuga de informação 78
Figura 26: Esquema da PEM impressa em papel (frente) 81

Figura 27: Esquema da PEM impressa em papel (verso) 81
Figura 28: Distribuição geográfica da amostra populacional 86
Figura 29: Respostas sobre as entidades interessadas nos dados das prescrições . 88
Figura 30: Respostas sobre as desvantagens da prescrição eletrónica 89
Figura 31: Respostas sobre o armazenamento dos dados das prescrições 89
Figura 32: Modelo do Cartão Profissional Eletrónico proposto 96
Figura 33: Encriptação de documentos a partir da chave simétrica do CPE 97
Figura 34: Proteção proposta dos dados das PEM 98
Figura 35: Esquema do Sistema Proposto de Prescrição Eletrónica 99
Figura 36: Modelo proposto da PEM impressa em papel 102
Figura 37: Exemplo de um QR-Presc e QR-Cert com 35 mm de lado 103
Figura 38: Computação da receita em QR-Code (Cryptool 2.0) 107
Figura 39: Sistema Proposto para o modelo físico da Prescrição Eletrónica 108

Índice de tabelas

Tabela I: Planificação da tese 12
Tabela II: Estado da Prescrição Eletrónica na Europa em 2010 62
Tabela III: Respostas às questões sobre segurança e privacidade dos dados 87
Tabela IV: Média de Idades e Desvio padrão das respostas sobre segurança e privacidade dos dados 87
Tabela V: Campos necessários para o processo de dispensa de uma PEM 104
Tabela VI: Capacidade máxima de dados de QR-Codes 106
Tabela VII: Campos do QR-Cert 110

Prefácio

A Prescrição Eletrónica de Medicamentos (PEM) projeta perspectivas de um sistema de gestão medicamentosa mais seguro, mas para o sistema ser funcional torna-se necessário o acesso imediato das informações dos utentes de várias entidades, o que levanta questões relativamente à privacidade, confidencialidade e segurança dos dados clínicos dos utentes. A menos que o Sistema de Prescrição Eletrónica (SPE) seja construído com os níveis de segurança apropriados, os benefícios retirados do mesmo podem pôr em causa problemas éticos relacionados com a partilha desses mesmos dados. [1]

A elaboração deste trabalho, revelou-se um desafio pessoal, uma vez que este foi realizado durante um período de permanentes alterações legislativas relativas à PEM, o que implicou uma constante revisão bibliográfica sobre a temática. Ao contrário do previsto, a necessidade de atualização revelou-se por um lado altamente motivante, quer por ver certos aspectos de segurança a serem corrigidos, mas por outro lado, a necessidade cada vez maior de realçar os aspectos de segurança esquecidos durante todo este processo de transformação do SPE.

1 Introdução

Desde a primeira receita eletrónica emitida em Portugal em 2004, ao abrigo da Portaria 1501/2002[2], foram várias as alterações regulamentares e tecnológicas introduzidas na última década. As condições eram simples: qualquer prescrição podia ser preenchida informática ou manualmente.

As prescrições de medicamentos podem ser classificadas em cinco grupos [3]:

- Medicamentos não sujeitos a receita médica;
- Medicamentos de receita médica não renovável;
- Medicamentos de receita médica renovável;
- Medicamentos sujeitos a receita médica especial;
- Medicamentos de receita médica restrita de utilização reservada a certos meios especializados.

Este trabalho incide sobre a prescrição sujeita a receita médica. Mas antes de nos debruçarmos sobre o atual sistema de prescrição é importante rever a história do Sistema Nacional de Saúde de Portugal e descrever o contexto atual.

1.1 Breve história do SNS

Antes de 1974, a saúde em Portugal ficava a cargo de várias instituições com raízes diferentes na história do País e cujas vias se sobrepunham [4]:

- Misericórdias, responsáveis pela gestão de grande parte das instituições hospitalares e de outros serviços distribuídos pelos país;
- Serviços Médico-Sociais (SMS), prestadores de cuidados médicos aos beneficiários da Federação de Caixa de Previdência;
- Serviços de Saúde Pública, responsáveis pela proteção da saúde (vacinações, proteção materno-infantil, saneamento ambiental);
- Hospitais estatais, gerais e especializados (principalmente localizados nos grandes centros urbanos);
- Serviços privados, dirigidos aos estratos socioeconómicos mais elevados.

Em 1971 começou-se a projetar um Serviço Nacional de Saúde (SNS): entretanto os hospitais das Misericórdias foram nacionalizados em 1975; o financiamento proveio do orçamento geral do estado em 1976 e em 1979 criou-se o SNS, que ainda hoje representa uma rede de órgãos e serviços prestadores de cuidados globais de saúde a toda a população, através da qual o Estado Português salvaguarda o direito à saúde (promoção, prevenção e vigilância) a todos os cidadãos portugueses. [4]

Definiu-se como objectivo primário do SNS a proteção da saúde individual e colectiva através da prestação de cuidados integrados de saúde, com a promoção e vigilância da saúde, a prevenção da doença, o diagnóstico e tratamento dos doentes e a reabilitação médica e social.

Em 1984 iniciou-se a integração dos centros de saúde com os postos médicos dos SMS e, com esta ação, foi implementada o SNS projetado. Este

foi constitucionalmente definido como universal, geral e tendencialmente gratuito (tendo em conta as condições económicas e sociais dos cidadãos) onde ficou definido como papel do Estado a orientação das suas ações para a socialização dos custos dos cuidados médicos e medicamentosos. A lei inicial admitia as convenções e ressalvava o sector privado, livre mas complementar. [5]

Em 1990, foi alterada a Constituição Portuguesa, onde o direito à proteção da saúde passaria a ser garantido pelo Sistema de Saúde, em vez do SNS. Esta modificação veio permitir acordos com entidades privadas e a gestão empresarial dos hospitais públicos. [5]

Em 2002, são introduzidas modificações profundas na Lei de Bases da Saúde [6] optando-se por um novo modelo de gestão hospitalar, aplicável aos estabelecimentos hospitalares que integram a rede de prestação de cuidados de saúde com os modelos de gestão de tipo empresarial: as Entidades Público-Privadas (EPE).

Em 2007, foi criada a Administração Central do Sistema de Saúde (ACSS), instituto público, dotado de autonomia administrativa e financeira que se responsabilizou por assegurar a gestão dos recursos financeiros e humanos, das instalações e equipamentos do SNS e por implementar as políticas, normas, regulamentação e planeamento em saúde, em articulação com as Administrações Regionais de Saúde (ARS).

A partir de 2010, o Governo Português aprovou a criação de uma empresa de prestação de serviços partilhados ao SNS: Serviços Partilhados do Ministério da Saúde, EPE (SPMS). [7] Com autonomia financeira, administrativa e empresarial, com supervisão e controlo do Ministério da Saúde e do Ministério das Finanças, estes serviços estabeleceram como

objectivo promover a eficácia e eficiência nas organizações ligadas ao SNS, relacionadas com o mercado de medicamentos, equipamentos e de serviços terapêuticos privados, de forma a assegurar a prestação de serviços partilhados ao nível de compras e logística, gestão financeira, recursos humanos especializados e sistemas de Tecnologias de Informação e Comunicação para as várias entidades que integram o SNS.

Em Abril de 2011, o governo português viu-se obrigado a pedir ajuda financeira ao Fundo Monetário Internacional e a Bruxelas, pela terceira vez em três décadas, tendo sido elaborado um Memorando de Entendimento sobre as condicionalidades da Política Económica [8] e um Programa de Estabilidade e Crescimento [9], de forma a estabelecer um orçamento de estado que permitisse a redução de custos. Estes eventos levaram à criação de várias medidas com o objectivo de reduzir os custos nos vários ministérios, incluído o da saúde. Uma das medidas consistiu na desmaterialização de todo o circuito administrativo do medicamento, de forma a reduzir os custos da prescrição e a combater a fraude, em vigor a partir de Agosto de 2011. [10]

A desmaterialização do processo de prescrição eletrónica permitiria ainda "aumentar a qualidade da prescrição e incrementar a segurança do circuito do medicamento", onde era "incentivada a informatização do sistema de saúde, estimulada a comunicação entre os profissionais das diferentes instituições e diminuído o risco de erro ou confusão na prescrição", enquanto se adquire mais informações sobre o circuito do medicamento, desencorajando a fraude. [11]

Neste momento, o sistema de saúde português é constituído por uma rede de cuidados de saúde primários, uma rede de cuidados hospitalares

(Centros Hospitalares, Hospitais Privados), Instituto Português de Oncologia e Instituições de Saúde Privadas. Os cuidados de saúde primários, por sua vez encontram-se organizados geograficamente em ACES (definidos pelo número de pessoas residentes) que podem compreender as seguintes unidades funcionais: [12]

- Unidades de saúde familiar (USF);
- Unidades de cuidados de saúde personalizados (UCSP);
- Unidades de cuidados na comunidade (UCC);
- Unidades de saúde pública (USP);
- Unidades de recursos assistenciais partilhados (URAP);
- Outras unidades ou serviços, propostos pela respectiva ARS e aprovados por despacho do Ministro da Saúde.

As instituições públicas, nomeadamente centros hospitalares e unidades de Cuidados de Saúde Primários intercomunicam através da Rede de Informação da Saúde (RIS) e, mais recentemente, usando a Plataforma de Dados de Saúde (PDS), implementada pelos SPMS, que introduziu o Resumo Clínico Único do Utente (RCU2) de forma a permitir aos profissionais de saúde o acesso à informação clínica relevante dos utentes em qualquer ponto do país desde o primeiro semestre de 2011. [13]

A própria Ordem dos médicos, preocupada com os níveis de segurança verificados a nível nacional, decidiu avançar com medidas de segurança que incluem a atribuição de cédulas profissionais com capacidade de assinatura digital. [14]

1.2 Contexto Atual

Nos últimos anos tem-se verificado um aumento da preocupação com a cibersegurança, quer a nível da comunidade europeia, quer a nível da comunidade portuguesa. Tal preocupação verifica-se nos resultados de um inquérito, realizado em Julho 2012 pelo Eurobarómetro, onde se refere que "os utilizadores da Internet estão muito preocupados com a cibersegurança". Em Portugal, num universo de mil entrevistados, os dados obtidos demonstram que 75% dos inquiridos afirmam estar mal informados sobre os riscos de cibercrime, 69% receiam ser vítimas de roubo de identidade, 77% concordam que o risco de ser vítima de um ato de cibercriminalidade aumentou em 2010 e 61% afirmaram não ter alterado nenhuma palavra-chave (password) de acesso a serviços on-line. [15]

Durante o ano de 2012, foram anunciadas várias reformas sobre a prescrição eletrónica, vinhetas médicas e dispensa eletrónica. No entanto, como foi explicado na contextualização histórica do SNS, o problema que se aborda nesta tese tem início com a desmaterialização do processo de Prescrição Eletrónica de Medicamentos (PEM) de uma maneira não controlada e sem os níveis de segurança que este exige.

A transmissão de dados no interior do SNS é assegurada pela RIS, que interliga os sistemas de apoio ao médico nos cuidados de saúde primários com os sistemas existentes nos meios hospitalares e nas várias entidades públicas da área da saúde. As instituições privadas, por se encontrarem excluídas da RIS, não podem realizar essa comunicação diretamente. Com a introdução da legislação, que obriga os profissionais de saúde a prescreverem electronicamente, levantou-se um problema relativo à

transmissão dos dados constantes nas prescrições que incide principalmente nas instituições desprovidas de uma ligação à SPMS.

A solução que o ministério da saúde encontrou e aplicou consistiu na abertura ao mercado de produtos de *software* de PEM que seriam certificados e responsáveis pela transmissão dos dados das prescrições médicas à ACSS. Esta medida levou a que inúmeras empresas (vinte e uma com declaração de conformidade) desenvolvessem a apresentassem soluções informáticas de Sistemas de Prescrição Eletrónica (SPE). [16]

Os contractos celebrados entre as empresas de software de PEM e os clientes prescritores exibem potenciais falhas, quer pelo excesso de informação exigida aos médicos prescritores, quer pela falta de clareza sobre a responsabilidade da garantia de privacidade dos dados introduzidos no sistema. Para a celebração do contracto são pedidas cópias do cartão da Ordem dos Médicos, que contém todas as informações profissionais necessárias para realizar uma prescrição, complementadas através do Cartão de Cidadão, onde constam todas as informações pessoais que confirmam a identidade do mesmo prescritor (Figura 1).

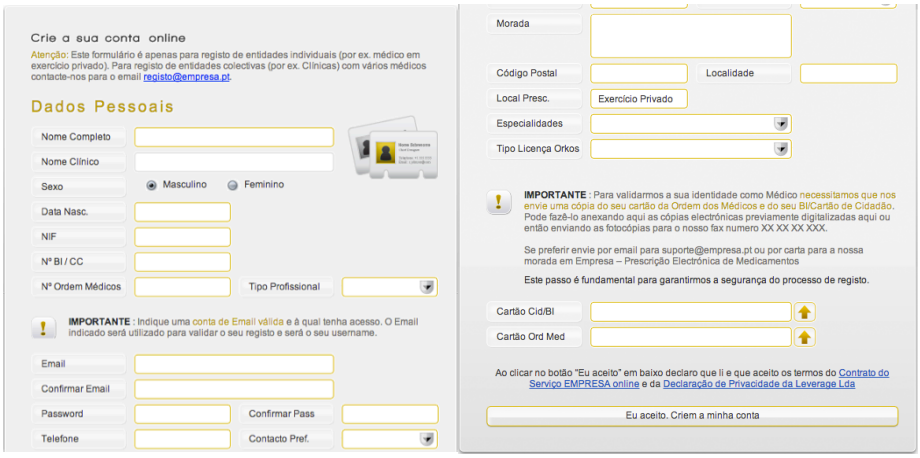

Crie a sua conta online
Atenção: Este formulário é apenas para registo de entidades individuais (por ex. médico em exercício privado). Para registo de entidades colectivas (por ex. Clínicas) com vários médicos contacte-nos para o email registo@empresa.pt.
Dados Pessoais
Nome Completo
Nome Clínico
Sexo
Masculino
Feminino
Data Nasc.
NIF
Nº BI / CC
Nº Ordem Médicos
Tipo Profissional
IMPORTANTE : Indique uma conta de Email válida e à qual tenha acesso. O Email indicado será utilizado para validar o seu registo e será o seu username.
Email
Confirmar Email
Password
Confirmar Pass
Telefone
Contacto Pref.
Morada
Código Postal
Localidade
Local Presc.
Exercício Privado
Especialidades
Tipo Licença Orkos
IMPORTANTE : Para validarmos a sua identidade como Médico necessitamos que nos envie uma cópia do seu cartão da Ordem dos Médicos e do seu BI/Cartão de Cidadão. Pode fazê-lo anexando aqui as cópias electrónicas previamente digitalizadas aqui ou então enviando as fotocópias para o nosso fax numero XX XX XX XXX.
Se preferir envie por email para suporte@empresa.pt ou por carta para a nossa morada em Empresa – Prescrição Electrónica de Medicamentos
Este passo é fundamental para garantirmos a segurança do processo de registo.
Cartão Cid/BI
Cartão Ord Med
Ao clicar no botão "Eu aceito" em baixo declaro que li e que aceito os termos do Contrato do Serviço EMPRESA online e da Declaração de Privacidade da Leverage Lda
Eu aceito. Criem a minha conta

Figura 1: Exemplo de formulário de inscrição numa empresa de software

Com acesso a estas informações, qualquer indivíduo pode registar-se em alguns produtos de software de PEM, que não exija um registo presencial ou autenticado (roubo de identidade), o que torna teoricamente possível a produção de prescrições eletrónicas "certificadas" por indivíduo não autorizados. Assim se potencia a usurpação da identidade digital e se procede de forma fraudulenta à prescrição eletrónica. O mesmo pode acontecer caso haja conhecimento das simples credenciais de acesso dos vários sistemas desenvolvidos.

Relativamente aos produtos fornecidos pelas empresas, a maioria destes são sob a forma de portais de internet e os seus utilizadores devem estar consciencializados que a informação introduzida na plataforma é armazenada no servidor da companhia de software ou, mais grave ainda, num servidor de outra companhia que não a contratada (conceito de *Cloud computing*), o que poderá por em causa a privacidade dos dados clínicos processados. A subcontratação de empresas é um negócio cada vez mais adoptado no mundo cibernético e a inexistência de regulamentação sobre este aspecto não impede que sejam contratados terceiros para fornecer os recursos necessários para várias empresas operarem no mercado.

De referir ainda que a cessação do contracto poderá igualmente ser mais complexa do que previsto e, embora existam cláusulas que obriguem ambas as partes a apagar os dados, não existe nenhum mecanismo de certificação deste processo.

Deter a informação nos dias de hoje corresponde a deter poder potencial, e o registo das prescrições pode revelar-se informação valiosa para muitas organizações, desde laboratórios farmacêuticos (com interesses na área dos medicamentos) até companhias de seguros,

instituições bancárias, ou mesmo simples empresas que pretendem recrutar novos funcionários (com interesse na área da prescrição que permitisse inferir a situação clínica do indivíduo).

A recente introdução das medidas legislativas relativas à prescrição eletrónica tem sido debatida entre as ARS, Ordem dos Médicos e Ministério da Saúde, temática que tem chamado a atenção dos órgãos de comunicação social desde o início do ano de 2012. [17-20]

O próprio Bastonário da Ordem dos Médicos, descreveu a atual situação como aterradora, depois de informado sobre empresas que armazenam indevidamente as informações dos utentes e que transmitem dados médicos de forma não encriptada. [16]

A Comissão Nacional de Proteção de Dados (CNPD) alertou para o enfraquecimento progressivo da relação médico-doente devido, à existência de intermediários no processo de prescrição eletrónica, e para a dificuldade em determinar o circuito da informação digital. Esta limitação no controlo da informação deve-se à existência de subcontratações de serviços (que podem ser realizadas recursivamente, podendo mesmo ser subcontratados serviços estrangeiros); à possibilidade de acesso remoto por parte dos técnicos de informática; e à incapacidade atual de identificar os indivíduos responsáveis pelo uso incorreto dos SPE [21]. A CNPD chamou atenção para o facto de os profissionais médicos não possuírem conhecimentos tecnológicos suficientes, pelo que é importante iniciar uma campanha de sensibilização que permita aos profissionais ter mais consciência sobre o atual sistema de prescrição e dos seus componentes. [20]

No ato de prescrição, os médicos são responsáveis pelo preenchimento de uma prescrição que é replicada sob uma forma digital (que é transmitida à ACSS) e uma forma material (impressão em papel) que é entregue ao utente, servindo como moeda de troca (*token*) numa farmácia, para ter direito a uma comparticipação por parte do estado.

Enquanto a privacidade dos dados na prescrição impressa fica ao cargo do próprio utente, a transmissão de dados eletrónica fica a cargo da RIS (no caso de se tratar de uma entidade do SNS) ou das companhias de *software* (no caso das companhias privadas).

A recente introdução da PDS (Plataforma de Dados de Saúde) também levanta algumas questões de segurança relativamente ao acesso dos dados dos utentes por parte dos profissionais de saúde. A nível dos cuidados de saúde primários, a consulta das informações clínicas (nomeadamente exames, diários médicos e relatórios) de qualquer utente inscrito na instituição onde os dados são consultados não depende nem da presença do utente, nem de um seguimento médico anterior, o que permite a qualquer profissional de saúde aceder a esses dados em qualquer momento, mesmo nunca tendo assistido o utente em questão.

Embora fosse referida a existência de um registo dos acessos aos dados dos utentes, a não existência de uma auditoria interna responsável pelo acesso aos dados, representa uma eventual fuga de dados [22]. Esta fuga de dados é preocupante, dado a intervenção de várias organizações no sistema que poderão ter interesse nas informações existentes nas prescrições eletrónicas e nas elações clínicas que destas é possível elencar.

1.3 Material e Métodos

A recolha de informações iniciais foi realizada com base numa revisão bibliográfica na Pubmed® realizada em Agosto de 2012 com base nos artigos que incluem as palavras chave *"Computer Security"[Mesh] AND ("Prescriptions"[Mesh] OR "Electronic Prescribing"[Mesh])* da qual foram encontrados 51 artigos. Após leitura dos resumos, foram selecionados 12 trabalhos de interesse, em inglês, cinco dos quais com acesso ao artigo completo. É interessante verificar que a maioria dos artigos pertence à Escandinávia, Reino Unido, Estados Unidos e Tailândia pelo que se pode inferir uma preocupação acrescida por parte destas sociedades.

Esta lista foi complementada com outros artigos sobre o tema procurados com o motor de busca Google®, com informações existentes na página da internet do ministério da saúde, ACSS e a legislação existente sobre a PEM em Diário da República (Figura 2).

O trabalho de investigação incluiu ainda a realização de um inquérito dirigido aos responsáveis pelos sistemas de prescrição das instituições de saúde privadas (profissionais de saúde ou não), aplicado a nível nacional constituído por perguntas de resposta fechada, realizado através da plataforma Medquest [23];

Os dados dos inquéritos foram analisados descritivamente e com cross-tables com auxílio do SPSS.

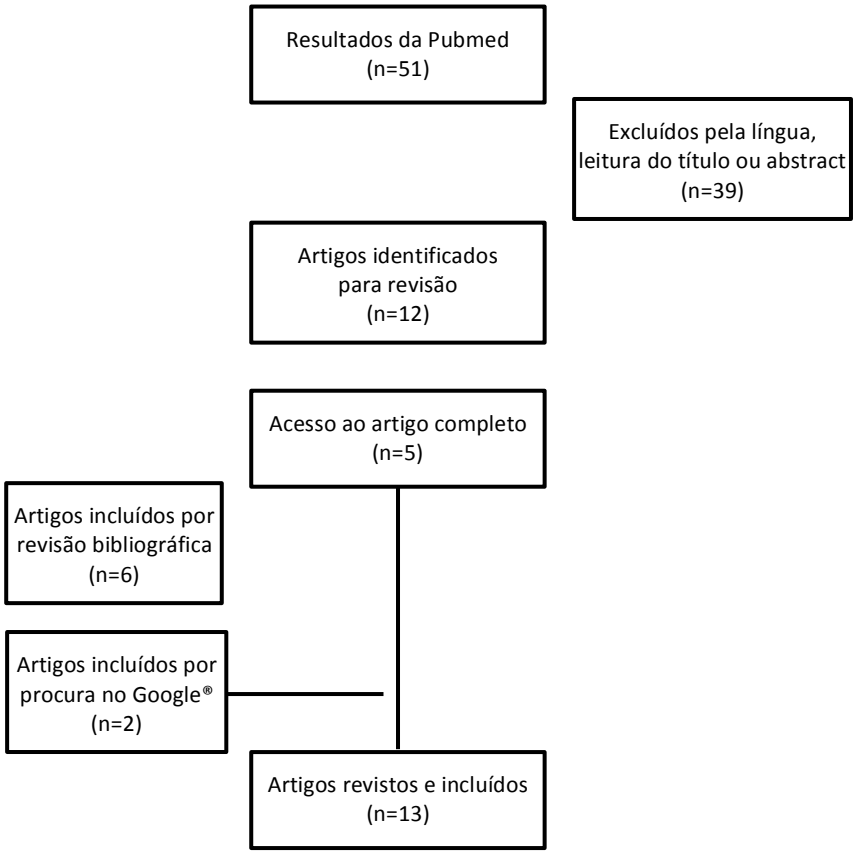


Figura 2: Métodos de Seleção de Artigos

Tabela I: Planificação da tese

	2012											2013	
	Jan	**Fev**	**Mar**	**Abr**	**Mai**	**Jun**	**Jul**	**Ago**	**Set**	**Out**	**Dez**	**Jan**	**Fev**
Pesquisa bibliográfica													
Realizar Inquérito Segurança													
Aplicar Inquérito Segurança													
Analisar Inquérito Segurança													
Descrição do Atual SPM e SPE													
Proposta de sistema de PEM													
Analisar Inquérito Europeu													
Comparar SPE na Europa													

Neste contexto surgiu a ideia de realizar este trabalho que se encontra dividido em quatro secções principais:

- Estado de arte com a descrição dos meios de segurança e as tecnologias atuais;
- Descrição do atual SPE e SPM, onde são identificando as várias falhas e os riscos subsequentes do sistema atual;
- Elaboração de um questionário aplicado a nível nacional aos responsáveis pelos uso dos sistemas de prescrição de instituições privadas, com o objectivo de avaliar o nível de percepção da segurança transmitida pelos atual sistema de prescrição e análise dos mesmos;
- Análise dos sistemas de Prescrição em vários países da Europa;
- Proposta de um sistema de prescrição capaz de corrigir as falhas encontradas e aumentar de uma maneira global os níveis de segurança, confidencialidade e privacidade dos dados pessoais dos médicos e dos utentes.

1.4 Trabalhos Realizados

À presente data, o autor apresenta os seguintes trabalhos elaborados no âmbito do mestrado:

- Participação no Prémio Ensaio da Comissão Nacional de Proteção de Dados com o trabalho "Privacidade dos Dados Clínicos", Lisboa, 2012;
- Apresentação oral do protocolo da tese "(in)Security in Electronic Prescription" no Simpósio de Informática Medica, Porto, 9/11/2012;
- Apresentação oral do artigo "Physician's awareness of e-prescribing security risks" no 26th IEEE International Symposium on Computer-Based Medical Systems, Porto, 20/06/2013;
- Apresentação oral intitulada "i-Society - Proposal of a Secure Electronic Prescription System" no congresso i-Society 2013, Toronto, Canadá, 24/07/2013;
- Apresentação do artigo "Benefits, Challenges and Impact of Teleconsultation - A Literature Review", como coautor, no congresso MedInfo 2013, Copenhaga, Dinamarca, 20/08/2013.

2 Estado de Arte

2.1 Privacidade, Confidencialidade e Segurança

De acordo com o Artigo 8 do capítulo de Direitos Fundamentais da União Europeia, relativo à proteção dos dados pessoais: todos os cidadãos têm direito à proteção dos seus dados pessoais; esses dados devem apenas ser processados para fins específicos e mediante o consentimento informado da própria pessoa (ou do seu representante legal legítimo); qualquer indivíduo tem direito a aceder aos dados pessoais recolhidos ou relacionados com o próprio.

Dale O'Brien e William Yasnoff, definem privacidade, confidencialidade e segurança de forma simples: *privacidade* é o direito de um indivíduo deter secretamente informação sobre ele próprio, sem conhecimento de outrem; a *confidencialidade* baseia-se na pressuposição que nenhuma informação capaz de identificar o indivíduo será revelada sem o consentimento do mesmo (excepto nos casos previstos pela lei); *segurança informática* representa o conjunto de mecanismos e infraestruturas que permitem a implementação e gestão de políticas de privacidade e confidencialidade num computador e sistema de telecomunicações. [24]

Uma eventual fuga de informação respeitante a um indivíduo, sem o consentimento do mesmo, representa um cenário de invasão à sua privacidade.

2.2 Segurança Eletrónica

Tendo em conta a crescente informatização que atualmente existe numa escala mundial, é importante assegurar que as comunicações se mantenham seguras e que os dados eletrónicos dos indivíduos que transitam se encontrem seguros nos vários sistemas que interagem entre si.

A definição de Segurança Eletrónica é um conceito multidimensional, que engloba os aspectos físicos de uma infraestrutura, pelas ligações que esta estabelece, pelos protocolos utilizados e pelas aplicações que esta executa. Dada a complexidade e conectividade dos sistemas de informação atuais, é praticamente impossível falar de um sistema de forma isolada sem considerar que este se encontra interligado a outros sistemas. Este fenómeno de rede obriga-nos a preocupar o máximo possível com qualquer sistema ou plataforma que se implemente ou que já esteja implementada (nomeadamente os sistemas de partilha de informação e de registo de informações clínicas e dos utentes), uma vez que o nível de segurança desta depende fortemente do nível de segurança do seu componente mais vulnerável.

Na área da saúde, o nível de segurança eletrónica baseia-se em cinco conceitos básicos [24-26]:

- Confidencialidade dos dados – garantir que a transferência e armazenamento dos dados dos utentes são confidenciais, impedindo o acesso não autorizado por indivíduos ou entidades não autorizadas;
- Privacidade dos dados – garantir que as informações sejam mantidas privadas para os intervenientes responsáveis e a sua transmissão ou visualização sejam consentidas por um utente devidamente informado das políticas de acesso em vigor;

- Integridade dos dados – certificar que um documento ou sistema eletrónico não sofre alterações, quer durante a transmissão, quer no momento em que é acedido, quer durante o perdurante que é mantido pelos sistemas de informação.
- Autenticidade dos dados – garantir que a identidade de todos os intervenientes num processo de introdução, modificação ou comunicação eletrónica de dados é validada de forma adequada de forma a garantir a origem e qualidade da informação gerida pelos sistemas de informação;
- Não repúdio – garantir que, durante a introdução, modificação ou envio de dados, nem o autor da introdução ou modificação possa negar a sua intervenção, nem os intervenientes na comunicação possam negar o seu envolvimento e acesso a uma determinada informação, assim como a data e o local a partir do qual esta foi acedida ou recebida.

2.2.1 Chaves Simétricas e Chaves Assimétricas

Antes de descrever o mecanismo de assinatura digital, é conveniente ter presente os conceitos de chaves simétricas e chaves assimétricas.

Até ao início da década de 70 para que duas pessoas pudessem comunicar de forma segura, não presencialmente, teriam que combinar previamente de forma presencial uma chave de cifra que mais tarde seria usada para cifrar e decifrar (chave simétrica) a mensagem. Uma chave simétrica representa uma chave que é usada simultaneamente para encriptar e desencriptar uma mensagem e este tipo de cifras são conhecidos como criptografia simétrica.

Existem vários tipos de algoritmos para este tipo de criptografia, tais como AES (explicado na secção seguinte), BlowFish e outras variantes do DES (Data Encrypt Standard) [27]. Tal é exemplificado na Figura 3, onde o indivíduo A e o indivíduo B terão que usar o mesmo método criptográfico e a mesma palavra-chave para que estando separados fisicamente possam usar um canal de comunicação inseguro para comunicar de forma segura.

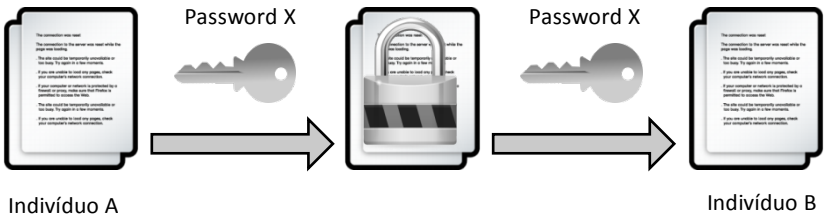


Figura 3: Exemplo de chave simétrica

Com a massificação das comunicações eletrónicas e a necessidade crescente de comunicar de forma segura com várias pessoas com as quais não existia nenhum encontro prévio, a criptografia simétrica apresenta algumas limitações a nível de gestão de chaves.

A criptografia assimétrica, ou de chave pública, surge na tentativa de resolver o problema da gestão de chaves. Nestes sistemas de cifra cada utilizador tem um par de chaves (ch_pública,ch_pública) com a característica de, a partir da chave pública, ser computacionalmente muito difícil obter a chave privada. O emissor usa a chave pública do recetor para cifrar a mensagem e só com a chave privada do recetor se consegue recuperar a mensagem.

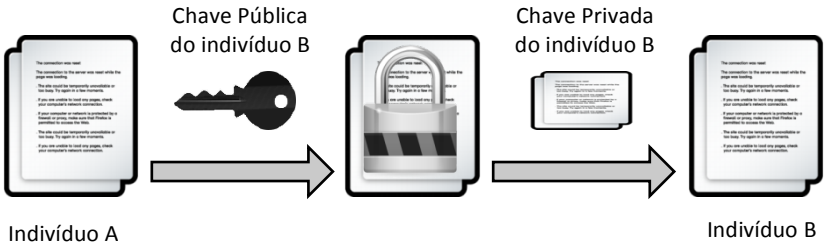


Figura 4: Exemplo de encriptação com uma chave Assimétrica

No exemplo descrito na Figura 4, a informação é cifrada com a chave pública do recetor e só pode ser decifrada pela sua chave par (chave privada) que está, unicamente, na posse do recetor legítimo das informações.

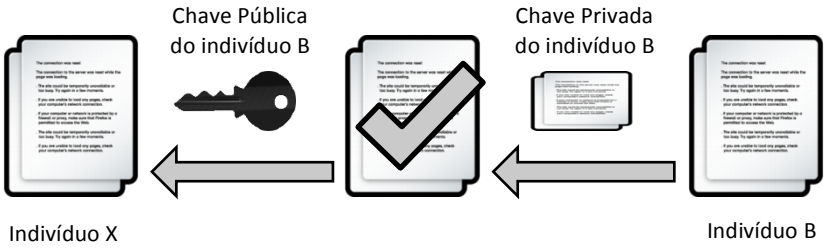


Figura 5: Exemplo de autenticação com uma chave Assimétrica

Outra das vantagens deste método verifica-se quando o processo se realiza no sentido oposto, ou seja, se o Indivíduo B aplicar a sua chave privada numa mensagem, qualquer outro indivíduo poderá assumir a mensagem como autêntica ou assinada digitalmente pelo individuo B, uma vez que só o indivíduo B possui a chave privada a que corresponde a mesma chave pública (Figura 5). Com este método é possível, por um lado cifrar informação usando a chave pública (Figura 4) e assinar usando a chave privada (Figura 5), mantendo a integridade dos dados.

Estas características permitem a elaboração de outros protocolos criptográficos com utilidade para transações financeiras, criação de chaves partilhadas, assinaturas digitais, aplicação de selos temporais, protocolos de não repudiação, etc.

Os algoritmos mais conhecidos de Chaves Assimétricas incluem o RSA e o DSS (Digital Signature Standard). O software PGP (Pretty Good Privacy) tornou-se popular pela implementação de chaves públicas e o OpenSSL pela gestão de chaves e certificados.

Atualmente são várias as empresas que lançam desafios à comunidade cibernética para tentar quebrar este tipo de cifras, como forma de certificar

a segurança dos protocolos criptográficos. A mais recente foi a quebra do RSA-768 bits realizada por um projeto que envolve uma rede mundial de milhares de utilizadores[*], que demorou cerca de 3 anos tendo envolvido cerca de 2000 processadores de 2.2Ghz. [28]

Quanto à segurança criptográfica, os sistemas informáticos podem ser, no sentido da informação:

- **Inseguros** – se os algoritmos usados podem ser decifrados com alguma facilidade;
- **Seguros no sentido da dificuldade computacional** – de acordo com a teoria da Complexidade, pode ser extraída do texto cifrado informação sobre o texto original mas os melhores algoritmos para esse fim demorariam um tempo proibitivo;
- **Seguros** – em que o conhecimento do texto cifrado não permite qualquer informação sobre o texto original, sendo por isso, em princípio, impossível decifrá-lo.

Esta experiência tem mostrado a inviolabilidade prática deste algoritmo criptográfico, em consideração que as chaves modernas são superiores a 1024 bits.

[*] http://www.distributed.net

2.2.2 Método DES e AES

Dada a evolução tecnológica e de telecomunicações na década de sessenta, surgiu a necessidade de apostar na área da criptografia e proteção dos dados eletrónicos.

Neste contexto histórico foi desenvolvido o DES (Data Encrypt Standard), entre 1972 e 1974. No início foi mantido secreto por várias agências governamentais americanas mas a sua publicação em 1975 fez com que se torna-se o algoritmo de chave simétrica padrão (Figura 6).

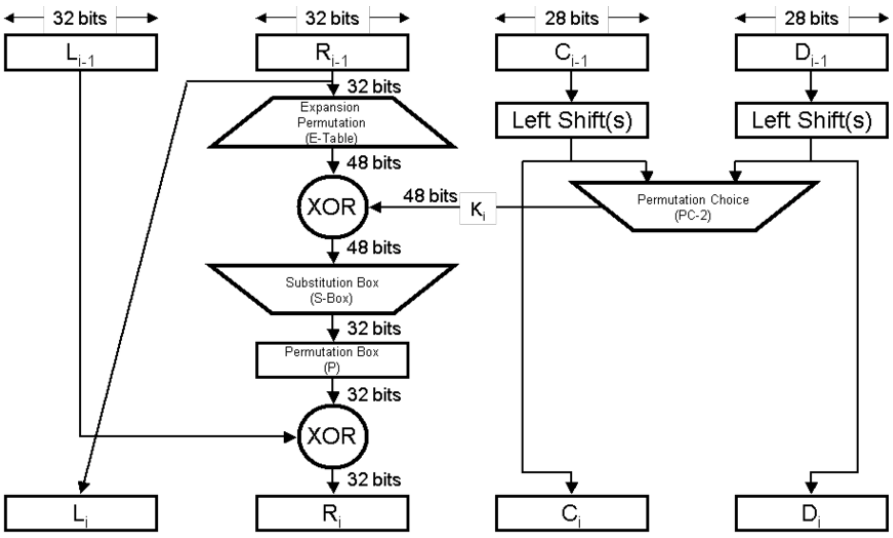


Figura 6: Processos de Encriptação e desencriptação com o algoritmos DES

O DES é uma cifra de bloco o que significa que a mensagem original é dividida em blocos de 64 bits (8 caracteres), sobre os quais é aplicada uma chave com as mesmas dimensões (composta por 56 bits mais 8 bits de paridade) que resultam num novo bloco cifrado de 64 bits.

Cada bloco é permutado (alteração da ordem da informação) em dois subgrupos e, durante 16 ciclos, cada bloco é transformado pela Função de Feistel, alternadamente, e novamente permutado. A própria é transformada com divisões e rotações de forma a gerar 16 subchaves de 48 bits que são usadas no ciclo correspondente. A Função de Feistel é constituída por quatro estágios: Expansão, Mistura de chaves, Transposição (XOR), Substituição (S-boxes) e nova Permutação. A ordem das transposições e substituições depende do valor da subchave anterior

Este algoritmo pode ser aplicado de diferentes modos:

- Electronic Code Book (ECB) - modo de encriptação nativa do algoritmo em que um mesmo bloco de texto vai ter o mesmo resultado cifrado;
- Cipher Block Chaining (CBC) - modo de encriptação sequencial em que o bloco cifrado inicialmente é usado como chave do bloco seguinte
- Cipher Feedback (CFB) - modo de encriptação sequencial em que existe um vector de inicial ao qual é aplicado o algoritmo de cifragem seguido de um XOR de onde se retiram bits usados no subgrupo seguinte;
- Output Feedback (OFB) - semelhante à CFB mas os bits são retirados diretamente do texto cifrado.

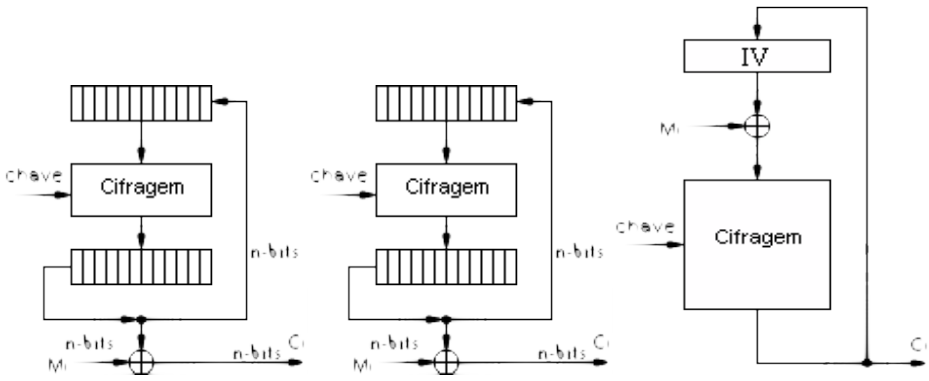


Figura 7: Esquema de funcionamento do DES (CBC, CFB, OBF) [29]

A evolução do poder computacional permitiu que os ataques por força bruta ao DES fossem cada vez mais rápidos e mais baratos (valores em dólares americanos) [29, 30]:

- em 1977 Diffi e Hellman propuseram uma máquina de vinte milhões de dólares capaz de quebrar o DES num dia;
- em 1993 Wiener propôs uma máquina semelhante com um custo de um milhão de dólares capaz de quebrar o DES em 7 horas;
- em 1997 o projeto DESCHALL quebrou o "DES challenge" (proposto pela RSA) em 96 dias usando o poder de computação de milhares de máquinas existentes na internet;
- em 1998 a Electronic Frontier Foundation (EFF), quebrou o DES (DES-cracker) com um custo de 250,000 USD;
- em 2006 o grupo COPACOBANA (Cost-Optimized Parallel Code Breaker) desenvolveu um dispositivo de baixo custo (10.000 dólares) capaz de quebrar o DES numa semana.

Em Janeiro de 1997 o National Institute of Standards and Technology (NIST) lançou um concurso mundial para encontrar um bom substituto para o DES a que chamou AES (Advanced Encryption Standard). Foram submetidas 15 cifras das quais foram selecionadas 5: MARS, RC6, Rijndael, Serpent, e Twofish. Em Outubro de 2000 o Rijandel foi selecionado como vencedor e em Novembro de 2001 tornou-se um standard oficial com o algorítmo AES [31]. O AES foi desenvolvido por dois criptógrafos belgas, Vincent Rijmen e Joan Daemen, que o batizaram de Rijndael (conjugação de ambos os apelidos) em 2000, esta cifra permite tamanhos de chave de 128, 192 ou 256 bits e tamanho de blocos de 128 bits [32]. Atualmente é um dos algoritmos de chave simétrica mais usados na comunidade cibernética.

2.2.3 Algoritmo RSA

O RSA (representação das iniciais dos apelidos dos autores, Rivest, Shamir e Adleman) é um algoritmo criptográfico de chave pública descrito pela primeira vez em 1978 [33] que tem sido progressivamente implementada nas últimas décadas de forma a promover a segurança nas trocas de informações confidenciais.

De uma forma sumária, pretende-se que a chave pública de cifra (***E***) seja usada para cifrar uma mensagem (***M***) de forma a ser decifrada usando uma chave privada (***D***). Estas chaves são complementares, sendo que a cifra sucessiva de uma mensagem ***M*** usando cada uma das chaves produz a mensagem inicial.

$$E(D(M)) = M \qquad D(E(M)) = M$$

A segurança deste algoritmo baseia-se na dificuldade computacional do problema da factorização de números grandes (valores superiores a 10^{300}). Note-se que do ponto de vista da complexidade computacional este problema não está classificado como NP-completo, i.e., um problema muito difícil nem é conhecido um algoritmo eficiente (não se sabe se pertence ou não a classe P) que o resolva. As implementações atuais mais vulgares usam chaves de 1024 e 2048 bits (sendo este último equivalente a um número primo de 617 dígitos). Uma vez que a factorização em números primos parece ser um problema computacionalmente difícil, torna-se muito moroso atacar este sistema a luz do conhecimento atual.

O processo de produção da chave pública e da chave privada, é feito a partir geração de dois números primos aleatórios (denominados de ***p,q***) dos quais se pretende obter dois valores (***d,e***) que serão usados para criar o par chave púbica (***N***,***d***) e o par chave privada (***N***,***e***).

O produto dos primos (***N*** = ***p*** x ***q***), é usado como módulo (e cujas dimensões correspondem ao tamanho da chave usada – por exemplo um módulo de 128 bytes corresponde a uma chave RSA de 1024). Com a aplicação da função de Euler (representada por **ϕ(p×q)=** (***p*** **-** 1) x (***q*** - 1). Do intervalo [1 , ϕ(***N***)] é retirado aleatoriamente um coprimo (ou seja, um número que não seja divisor de ϕ(***N***), que corresponderá ao expoente ***e***.

$$\phi(N) = (p - 1) \times (q - 1)$$

$$\phi(N) \perp e$$

A chave pública é associada com o par de valores ***N,e***. A mensagem cifrada é calculada a partir do valor da mensagem (***M***) elevado a ***e***, ao qual é aplicado o módulo ***N*** (ou seja o resto da divisão de M^e por ***N***).

$$C = E(M) = M^e \pmod N$$

Para criar a chave privada, usa-se o mesmo ***N***, mas com um expoente diferente ***d*** (geralmente do mesmo tamanho do módulo, ou seja, 128 bits) obtido a partir do módulo de ϕ(***N***) aplicado ao inverso de ***e***.

$$\boldsymbol{d} \equiv \boldsymbol{e}^{-1} \bmod (\phi(\boldsymbol{N}))$$

A chave privada é associada com o par de valores ***N,d***. A mensagem original é calculada a partir do valor cifardo (***C***) elevado a ***d***, ao qual é aplicado o módulo ***N*** (ou seja o resto da divisão de $\boldsymbol{M^d}$ por ***N***).

$$\boldsymbol{M} = \boldsymbol{D}(\boldsymbol{C}) = \boldsymbol{M^d \ (mod\ N)}$$

N (porção comum das chaves)
14393256779886593024999370662531983368051506908766552794469424123950735463075272798080821229850794595127100945990683746758222755029991803078504453757432152816709367010801545080403412965778146463076031583172228710278697054821814993616656586790918635702927185525001289313836351165957004942342141090387525327718 1

e (parte pública da chave)
65537

d (parte privada da chave)
12457742917470850096129885430542506134997843628681110528609542914795939979057353467481521940919731947052652304200307381343568176088640844680487154354587199600348459943874473981240036379075684544862485099708336309345371275171682720470485484486027524930018720615239001561897788066108504714967217982778905541785 7

Figura 8: Exemplo dos componentes necessários para gerar uma chave RSA

Como explicado anteriormente, de acordo com a teoria da Complexidade, este algoritmo é considerado seguro no sentido da dificuldade computacional uma vez que tem como base funções polinomiais. Esta última caraterística significa que uma determinada função é facilmente calculada (f(x) em termos de |x|) mas já o inverso não é possível não pode ser calculada em tempo polinomial (f^{-1}(y) em termos de |y|). O segredo desta propriedade encontra-se no produtos de números primos **(p×q)**, operação matemática realizada com facilidade, ao contrário

da fatorização em primos para a qual não se conhece nenhum algoritmo que resolva eficientemente esse problema. Por esse motivo se chamam a estas funções polinomiais, funções "*one-way*" por só permitirem (em tempo polinomial) calcular numa determinada direção.

Este algoritmo criptográfico tem várias vantagens:

- é eficiente em tempo real;
- pode ser executado por um computador ou *smartcards*;
- não implica partilha da chave privada (que fica sempre na posse do proprietário);
- dadas as combinações possíveis e o uso de números primos, torna-se quase impossível de ser quebrado, a menos que seja descoberto de um novo algoritmo de factorização eficiente.

Permite também garantir as seguintes características:

- Cifra - com o uso da chave pública, apenas o dono da chave privada possa decifrar a informação usando a chave primária;
- Autenticação dos dados - com o uso da chave privada, que permite a confirmação da autoria dos dados por parte de qualquer individuo que use a chave pública.

2.2.4 Assinaturas

Do ponto de vista semântico, assinatura representa uma qualquer marca usada por um indivíduo (geralmente relacionada com o próprio nome ou pseudónimo), usada para validar um documento ou produto da autoria do próprio.

Na área médica, a assinatura ou rubrica serve constantemente para validar qualquer documento manuscrito ou impresso que contém dados do utente, pareceres médicos, pedidos de tratamentos, declarações ou outras ações realizados por outrem. Para além destas funções, é usada maioritariamente no ato da prescrição, quer manual, quer eletrónica.

A aplicação da assinatura digital surgiu como meio de substituir a assinatura manuscrita, de forma a permitir a transação eletrónica de informação. Durante o processo de assinatura de um documento, o autor é obrigado a confirmar a operação. A legislação portuguesa prevê a utilização de assinaturas digitais desde 2003 como uma "modalidade de assinatura eletrónica avançada baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública" [34]. De acordo com o artº 7º do DL 62/2003:

A aposição de uma assinatura eletrónica qualificada a um documento eletrónico equivale à assinatura autógrafa dos documentos com forma escrita sobre suporte de papel e cria a presunção de que:

- A pessoa que apôs a assinatura eletrónica qualificada é a titular desta;
- A assinatura eletrónica qualificada foi aposta com a intenção de assinar o documento eletrónico;

- O documento eletrónico não sofreu alteração desde que lhe foi aposta a assinatura eletrónica qualificada.

A aposição de assinatura eletrónica qualificada substitui, para todos os efeitos legais, a aposição de selos, carimbos, marcas ou outros sinais identificadores do seu titular.

De acordo com o Artigo 3º do DL 62/2003 quando lhe seja aposta uma assinatura eletrónica qualificada certificada por uma entidade certificadora:

- o documento eletrónico tem a força probatória de documento particular assinado, nos termos do artigo 376.o do Código Civil.
- o documento eletrónico cujo conteúdo não seja suscetível de representação como declaração escrita tem a força probatória prevista no artigo 368.o do Código Civil e no artigo 167.o do Código de Processo Penal.
- O valor probatório dos documentos eletrónicos aos quais não seja aposta uma assinatura eletrónica qualificada certificada por entidade certificadora é apreciado nos termos gerais de direito.

Uma vez que estas se baseiam num sistema de encriptação assimétrico (o que exige um poder de computação acrescido), a aplicação prática das assinaturas digitais, como mecanismo de autenticação da autoria dos dados, incide sobre um resumo dos documentos em que é aplicada (denominada *hash* e cujas dimensões geralmente não ultrapassam os 512 bits) como se exemplifica na Figura 9. Desta forma, é muito mais eficiente cifrar esta pequena quantidade de informação (resumo) que, depois de confirmada a assinatura, é comparada com um novo resumo obtido do documento enviado. Se o resumo assinado coincidir com o resumo decifrado, podemos asseverar que o documento não foi alterado e que o

autor é inequivocamente o proprietário da assinatura (mecanismo de autenticação e não repúdio). A função que calcula o resumo é conhecida publicamente e deve ser resistente a colisões, i.e., deve ser extremamente improvável que dois documentos diferentes originem o mesmo resumo. As assinaturas digitas são verificáveis publicamente, transferíveis e garantem o não repúdio.

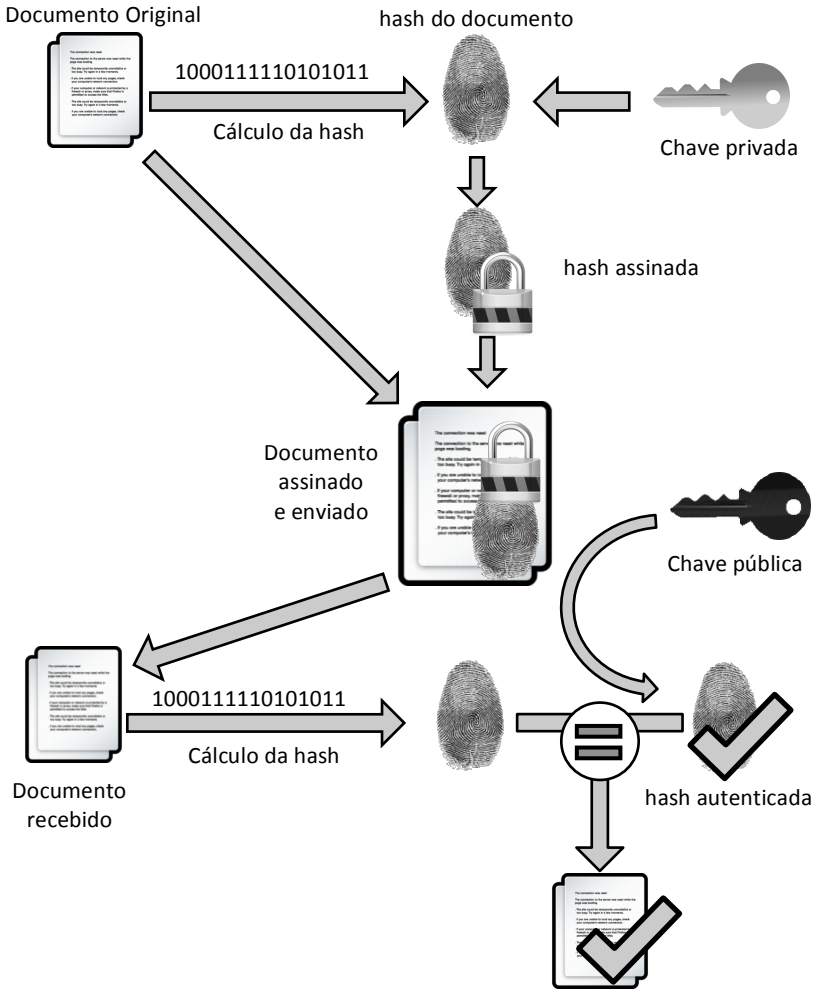


Figura 9: Assinatura da *hash* de um documento

Estas assinaturas têm a mesma validade que as assinaturas manuscritas, desde que se baseiem em certificados emitidos por entidades certificadoras credenciadas, tópico que será abordado na secção seguinte.

De uma forma sumária, as assinaturas digitais têm a vantagem de:

- identificar de forma unívoca o titular como autor do documento;
- serem aplicadas apenas após confirmação do autor;
- estabelecer uma conexão ao documento de forma a detectar qualquer alteração que este sofra desde o remetente até ao destinatário.

2.2.5 Assinaturas de Grupo

Dentro dos vários tipos de assinaturas digitais, existem as assinaturas intermediárias (proxy signature) que permitem a certificação de um indivíduo por um terceiro interveniente no processo, através da delegação do certificado deste e assinaturas de grupo (group signatures), que permitem que a autenticação e anonimato das informações. Este último modelo foi introduzido por David Chaum and Eugène Van Heyst em 1991 [35] de forma a possibilitar a autenticação dos dados transmitidos e, simultaneamente, o anonimato dos indivíduos, uma vez que os destinatários apenas conseguem identificar o grupo/organização a que este pertence (Figura 10).

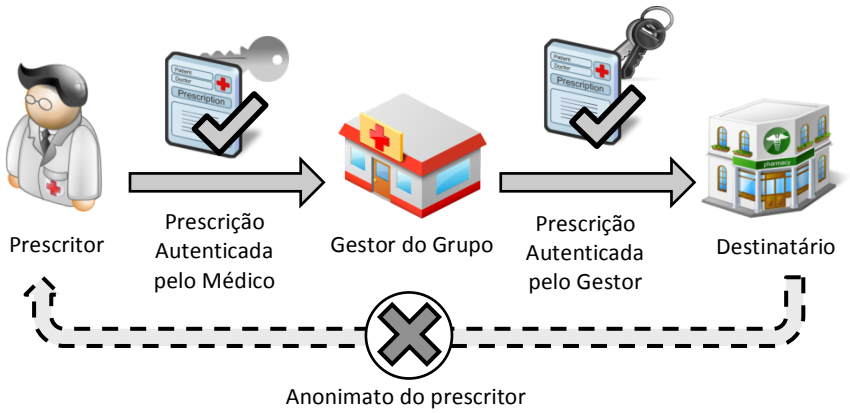


Figura 10: Exemplo de criação de uma chave de grupo

Cada grupo é detentor de uma chave de grupo pública e uma chave de grupo privada, controladas pelo gestor do grupo. Cada membro possui de igual modo uma chave pública e uma chave privada emitidas pelo gestor do

grupo ou outra entidade associada. Desta forma, com a intervenção do gestor neste processo, é possível rastrear a identidade de cada elemento.

Resumidamente, este modelo apresenta três propriedades fundamentais:

- apenas os membros podem assinar em nome do grupo;
- o destinatário consegue verificar a validade da assinatura do grupo mas não tem acesso ao autor da informação;
- caso seja necessário apurar responsabilidades, é possível identificar o autor original.

Do ponto de vista da segurança, este método tem-se revelado fiável por evitar a associação dos autores, manter o não repúdio, ser resistente à colisão de identidades e à prática de fraude. [36] Mais recentemente podemos encontrar referências a possíveis implementações deste método na área da saúde apresentado. [37, 38]

2.3 Infraestrutura de Chaves Públicas

Para funcionar com um multiplicidade de chaves assinaturas digitais, torna-se imprescindível a existência de um sistema capaz de criar, gerir, armazenar, confirmar, propagar e revogar as chaves públicas. [39]

Este sistema denominado PKI (*Public Key Infrastructure*) é formado por múltiplos componentes legislativos/jurídicos, que constituem uma infraestrutura física dotada de tecnologia, recursos humanos, normas, regulamentos e procedimentos que definem as políticas de certificação usadas com as assinaturas digitais. Analogicamente corresponde a uma base de dados ou um chaveiro de chaves públicas que se encontram associadas de forma segura ao seu titular de forma a garantir a sua veracidade.

Para além dos utilizadores e das suas respectivas chaves, uma PKI é geralmente constituída por uma cadeia de certificação com referências do emissor e destinatário do certificado, composta por diferentes tipos de entidades de certificação (CA – *Certification Authority*):

- Autoridade de Certificação de Raiz – organização de renome mundial que emite certificados a outras entidades e são incorporadas na maioria dos sistemas operativos;
- Entidades de Certificação Intermediária (ICA – *Intermediate Certificate Authority*) – entidades certificadas pelas Autoridade de Certificação de Raiz ou por outra ICA, que facilitam o processo de autenticação e correspondem aos elos centrais de uma cadeia de certificação;
- Autoridades de raiz de certificação de terceiros (TTP – *Trusted third party*) – usadas para facilitar as interações entre duas entidades que

analisam as comunicações entre ambas com o fim de prevenir transações fraudulentas.

Dentro de cada entidade há bases de dados (repositórios) onde são geridas as assinaturas válidas e as assinaturas não válidas: Repositórios de Certificados e Listas de Revogação de Credenciais (CRL – *Credential Revocation List*).

Existem vários modelos de PKI, assim como normas, sendo o formato X.509 bastante difundido na comunidade cibernética. Este modelo permite a identificação de um indivíduo a partir de um identificador (como correio eletrónico, endereço de DNS ou *smartcard*) que passa a ser representado por um certificado público, e simultaneamente recorre a Entidades de Certificação para confirmar a veracidade das identidades e Listas de Certificados Revogados (para definir os "certificados *non-gratos*") a partir de servidores OCSP (Online Certificate Status Protocol), que mantêm atualizada uma lista de certificados/revogações e devolvem uma resposta assinada sobre a validade do certificado inquirido que se limita a "válido", "revogado" ou "desconhecido" [40]. Uma vez que este protocolo se encontra atualmente implementado na maioria dos sistemas operativos, e foi assumido como padrão para o uso dos cartões de identificação em Portugal, pode representar uma facilidade na implementação das PKI.

Este sistema hierárquico, ao permitir uma propagação e revogação dos certificados, garante constantemente a integridade dos dados relativos à identidade dos indivíduos (Figura 11).

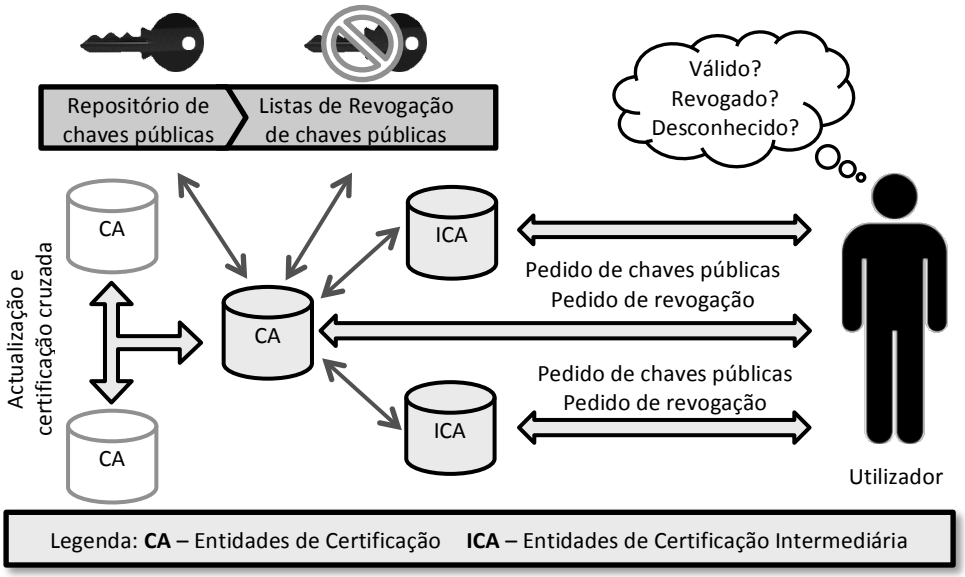


Figura 11: Representação de uma PKI (*Public Key Infrastructure)*

Foram definidas várias normas de funcionamento, sendo a mais comum o PKCS (Public-Key Cryptography Standards) definida pela empresa norte americana *RSA, The Security Division of EMC*. Na verdade, esta norma é composta por uma série de funções acessíveis apenas por programação que recorre a componentes de hardware (neste caso, *smartcards*, leitores e computadores), e a diferentes formatos pré-definidos (como chaves RSA, certificados X.509, chaves simétricas DES, etc), existindo 15 subnormas diferentes. A PKCS#11 ou *Cryptoki*, conhecida pelas suas potencialidades relativamente uso de certificados e chaves público-privadas tornaram-se módulos de uso frequente nos exploradores de páginas de internet, assim como nos *middlewares* (programas intermediários que permitem a autenticação dos utilizadores em sistemas e programas informáticos). Um exemplo de uso destas normas verifica-se no cartão de identificação

recentemente implementado em Portugal (Cartão de Cidadão) [41], como será explicado no seguimento deste capítulo.

Embora estas infraestruturas não sejam vitais para o uso individual de assinaturas digitais, tornam-se um pilar na gestão de assinaturas numa comunidade.

Em termos legislativos [34, 42, 43], em Portugal está definido que a assinatura digital tem a mesma autenticidade que um documento assinado em papel e que quem a pretenda usar "deve (…) gerar ou obter os dados de criação e verificação de assinatura, bem como obter o respectivo certificado emitido por entidade certificadora".

A gestão das assinaturas digitais em Portugal está dependente do SCEE que assume como objectivos "assegurar a unidade, a integração e a eficácia dos sistemas de autenticação digital forte nas relações eletrónicas de pessoas singulares e colectivas com o Estado e entre entidades públicas" [42]. Todavia, a legislação relativa a esta entidade foi recentemente revista em 2012 apenas para reformular a orgânica da gestão departamental. [44]

2.4 Smartcards

A necessidade de manter a chave privada segura, apenas acessível ao proprietário e para a qual é possível dar garantias fortes de que existe apenas um exemplar, coloca uma nova questão de segurança e de usabilidade: Onde se poderá armazenar a chave privada de forma segura e garantir unicidade de cópia sem comprometer em demasia a usabilidade do sistema? Uma hipótese de baixo custo, mas pouco segura, seria a de armazenar a chave privada num ficheiro ou até como um objecto de sistema, protegido dentro do próprio sistema operativo do computador. No entanto, uma vez que na prática existe a forte possibilidade das estações de trabalho serem partilhadas, não se pode assegurar de forma segura que o ficheiro ou o próprio objecto do sistema onde é guardada a chave privada nunca possa vir a ser copiado por um atacante. A forma normalmente adoptada para mitigar este risco consiste em armazenar a chave privada diretamente num dispositivo de segurança físico pessoal, intransmissível, transportável pelo utilizador e capaz de proporcionar os níveis de proteção adequados a uma chave privada sensível. Nomeadamente garantir que durante o seu tempo de vida útil a chave reside sempre dentro do dispositivo, e que em circunstância alguma essa chave sai para fora do controle direto desse dispositivo. Para este tipo de cenários é normal empregar *smartcards* ou outro tipo de *tokens criptográficos* seguros, capazes de gerar por eles próprios os pares de chaves e fazer com que seja extremamente difícil para não dizer impossível extrair a chave privada do desse dispositivo de segurança. Note-se que deste modo todas as operações criptográficas que envolvam essa chave privada protegida terão

que ser asseguradas pelo próprio dispositivo de segurança, uma vez que só ele lhe tem acesso.

Os *smartcard*s geralmente aparecem sob a forma de cartões de plástico, com dimensões correspondentes a 85.60 × 53.98 mm. Como exemplo temos os cartões multibanco e cartões de crédito com chip, documentos de identificações electrónicos e outros tipos de cartões cumpridores das normas de características físicas ID-1 ISO/IEC 7810 [45]. Este tipo de cartões tem sido associado a tecnologias de radiofrequência (ISO/IEC 14443 [46], sendo a norma MIFARE uma das tecnologias mais utilizadas atualmente para controlo de acesso físico a edifícios. Os smartcards aparecem normalmente sob a forma de cartões de plástico, contendo pequenos microprocessadores (ISO/IEC 7816 [47]) inseridos num chip com aproximadamente 1,27 cm de diâmetro. Este permite a conexão a leitores de cartões eletrónicos que, para além de fornecerem a energia necessária para o funcionamento do microprocessador, permitem a interação com esse dispositivo, enviando e recepcionando dados através de protocolos de comunicação pré-estabelecidos ([48]).

A ideia de associar um microprocessador a um cartão de plástico foi inicialmente concebida pelos engenheiros Helmut Gröttrup e Jürgen Dethloff em 1969. Esta foi patenteada em 1978 [49] após ter sido criado o primeiro microprocessador específico para estes cartões por Michel Ugon em 1977.

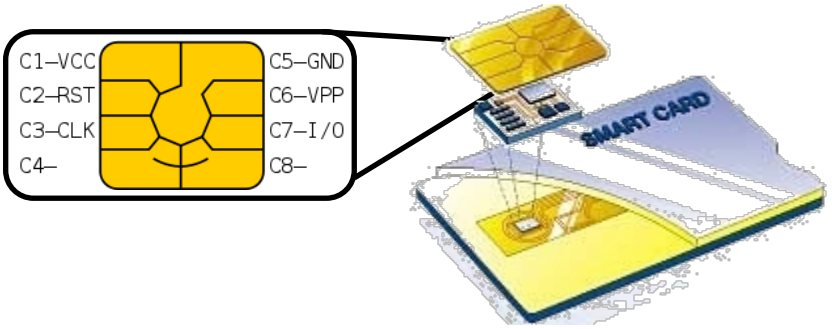


Figura 12: Exemplo de um smartcard, o chip interno e dos seus conectores

Uma das vantagens dos *smartcards* é o facto de não necessitarem de baterias (a energia necessária é fornecida pelo próprio leitor) e de possuírem uma memória *EEPROM* (Electrically Erasable Programmable Read-Only Memory) que mantém em segurança as informações guardadas durante a ausência de energia.

Outra capacidade de processamento dos micro processadores é o uso da tecnologia *"Java Card"*, que permite a programação, execução e implementação de aplicações desenvolvidas em ambiente Java™ (applets) nos circuitos do cartão. Desta forma é possível executar os applets num ambiente seguro (no interior do cartão), recurso que tem hoje diversas aplicações tecnológicas: Telecomunicações, Finanças, Governo, Identificação eletrónica, pagamento de serviços, etc. [50]. O desenvolvimento de applets capazes de efetuar operações criptográficas de forma estandardizada com certificados X509 e outras normas baseadas no standard PKIX no interior do próprio chip do *smartcard* [48], garante a operacionalidade do par de chaves sem que em momento algum a chave privada tenha que ser extraída para fora do chip do cartão. A memória EEPROM é apenas acessível após a introdução de um código PIN (chave

simétrica) que desbloqueia o uso da chave privada no processamento de dados provenientes do computador. O isolamento do processamento da chave privada no interior do smartcard garante que a mesma não seja exportável ou duplicada.

As funcionalidades criptográficas que envolvem a chave privada só se tornam acessíveis após a introdução de um código PIN (chave simétrica), que desbloqueia o uso da chave privada no processamento de dados provenientes do computador diretamente pelo *smartcard*. O isolamento do processamento da chave privada no interior do *smartcard* garante que a mesma não seja nunca exportável e/ou duplicada.

Como apresentado na Figura 9 (página 33), a assinatura é realizada sobre a sumarização criptográfica de um documento (*hash*), sendo apenas devolvida pelo cartão a sequência binária da assinatura digital que é anexada ao documento original, ficando este marcado como assinado. Qualquer alteração realizada ao documento irá resultar em alterações do *hash* do mesmo, que deixará assim de ser idêntico ao *hash* assinado.

2.4.1 Cartão de Cidadão

Em Portugal iniciou-se um processo de atribuição de cartões de identificação (Cartão de Cidadão (CC)) em 2007 com o objectivo substituir de bilhete de identidade (de momento simultaneamente em vigor) e integrar outros documentos: cartão de contribuinte, cartão de beneficiário da Segurança Social, cartão de utente do Serviço Nacional de Saúde e cartão de eleitor. O CC permite a identificação do proprietário do ponto de vista físico (como cartão) e eletrónico (através da assinatura digital autenticação forte), sendo aceite internacionalmente dentro da União Europeia.

Com este trabalho pretendemos dar início a uma eventual especificação dos atributos de identidade necessários para um documento de identificação para profissionais de saúde, com características semelhantes ao CC, com qualificação profissional. Para isso é importante perceber o modo de funcionamento do CC e quais as funcionalidades que este possui para poder efetuar assinaturas digitais com validade legal e poder ser utilizado como factor de autenticação de nível dois, em contextos onde é importante garantir propriedades fortes de não repúdio.

Tal como a maioria dos *smartcards*, o CC é um Java Card que segue as normas ISO 7810 e ISO 7816-2, anteriormente referidas, [51] e apresenta um aspecto gráfico de acordo com a **Error! Reference source not found.**. Na face principal, anverso, apresenta uma fotografia do indivíduo obtida durante o processo de registo, e contém de forma legível o Apelido(s), Nome(s), Sexo, Altura, Nacionalidade, Data de Nascimento, elementos de identificação civil (Nº Documento, Data de Validade e Assinatura do Titular). No verso descreve a filiação e os números de identificação Fiscal, Segurança

Social, número de utente do SNS, versão do cartão na lateral esquerda e, na região inferior, uma zona de leitura ótica relativos aos dados impressos na frente do cartão.

Figura 13: Cartão de Cidadão (frente e verso)

De acordo com o manual de especificações dos Leitores do CC, o chip do cartão apresenta as seguintes características [48]:

- Suporta a norma Java Card e o uso de logical channels;
- Possui uma capacidade de memória EEPROM (ou equivalente) mínima de 64 KB;
- Possui capacidades de gestão de memória dinâmica, suportando garbage collection pela JVM e de proteção de memória;
- Possui capacidades de gestão de espaço de armazenamento, incluindo desfragmentação e reutilização de espaço libertado;
- Possui capacidades de true random number generation;
- Suporta múltiplos PIN, em conformidade com a norma ISO/IEC 7816-4;
- Suporta mecanismos de bloqueio em caso de erro na introdução do PIN após 3 tentativas e respectivo desbloqueio por meio de introdução de PUK do cidadão e de chave administrativa de acesso ao cartão, para desbloqueio;

- Suporta mecanismos de geração de novo PIN do cidadão, em caso de esquecimento deste, mediante a introdução do PUK do cidadão e do PUK aplicacional de geração de PIN;
- Possui um motor criptográfico interno que suporta:
  - assinatura e verificação RSA de 1024 bits;
  - assinatura eletrónica qualificada segundo a norma CEN CWA 14169 (Secure Signature-creation devices "EAL 4+");
  - DES e TDES (triple Data Encription Standard);
  - MD5, SHA-1 e SHA-256, no mínimo;
  - MAC (message authentication code);
  - PKCS#1 (RSA Cryptography Standard) e PKCS#15 (Cryptographic Token Information Format Standard);
  - é compatível com leitores de cartões da norma EMV-CAP, para funcionamento de autenticação multicanal baseada em *one-time password*;
- Possui uma chave de proteção da personalização inicial;
- Está preparado para resistir aos ataques conhecidos do tipo "hardware attack", "timing attack", "simple power analysis" e "differential power analysis" entre outros.

No interior do chip estão armazenadas as seguintes informações [51]:

- a informação visível no cartão (com exceção da assinatura manuscrita);
- data de emissão e a entidade emissora;
- morada (protegida pelo código PIN da morada);
- uma chave (privada) para autenticação do proprietário nos vários sistemas informáticos (protegida pelo código PIN da autenticação);

- uma chave (privada) para assinar documentos de forma a possibilitar o não repúdio (protegida pelo código PIN da assinatura);
- dois certificados digitais (chaves públicas) complementares às chaves privadas;
- dados sobre a impressão digital (apenas para validação da impressão digital do indivíduo obtida a partir de um sensor biométrico);
- um campo de 1000 caracteres alfanuméricos editável.

Ao todo possui três códigos PIN, que são independentes e configuráveis. Só após a introdução dos códigos PIN corretos é que é permitido o acesso aos diferentes módulo e às suas respectivas funcionalidades e informações protegidas. As chaves privadas nunca abandonam os módulos (applets) do chip em que estão implementadas. Assim as informações são enviadas pelo leitor e processadas no interior do chip. A introdução dos códigos PIN pode ser realizada através de software (por meio da API disponibilizada na portal do cartão de cidadão – http://www.cartaodocidadao.pt) ou com a utilização de leitores com teclado numérico.

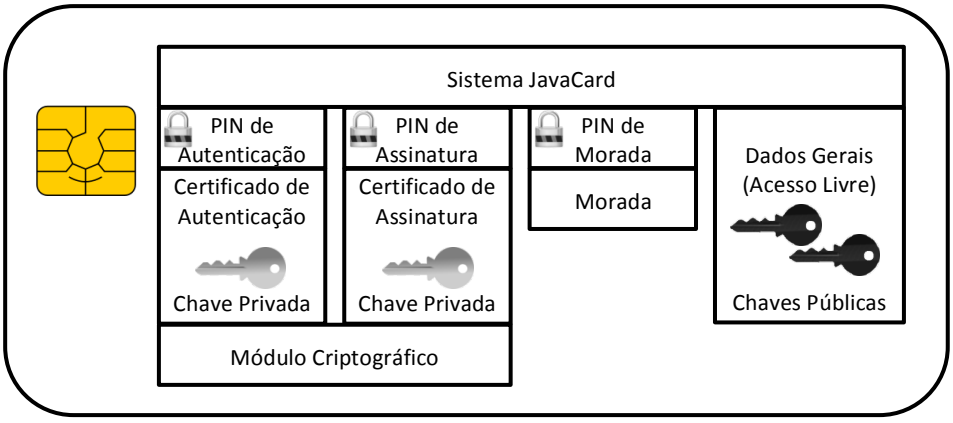


Figura 14: Informação contida no Cartão de cidadão

Relativamente aos pares de chaves assimétricas geradas pelo cartão aquando da sua inicialização, cada uma apresenta uma segurança de 1024 bits, e são assinadas pelo Sistema de Certificação Eletrónica do Estado (SCEE) cujo certificado se identifica como "ECRaizEstado" [42], que por sua vez é certificado e emitido pela "GTE CyberTrust Global Root", uma entidade certificadora de raiz com atribuição de confiança internacional. O certificado ECRaizEstado autentifica o "certificado Cartão de Cidadão 001" (atualmente existe apenas um certificado válido até 2019) que por sua vez é responsável pela autenticação dos certificados "EC de Autenticação do Cartão de Cidadão xxxx" e "EC de Assinatura Digital Qualificada do Cartão de Cidadão xxxx" (atualmente existem sete certificados, emitidos anualmente desde 2007). Esta hierarquia de certificação digital está representada esquematicamente na **Error! Reference source not found.**.

A SCEE corresponde a uma Entidade de Certificação intermediária que garante a segurança eletrónica do Estado Português e a autenticação digital forte das transações eletrónicas entre os vários serviços e organismos da Administração Pública e entre o Estado e os cidadãos e as empresas.

Os certificados emitidos encontram-se em formato X.509 v3, sendo o Ministério da Justiça o responsável pelas funções de repositório da Entidade Certificadora do Cartão de Cidadão e pela publicação do estado dos certificados emitidos e revogados por meio dos OCSP (Online Certificate Status Protocol), e qualquer certificado emitido fica armazenado durante um prazo mínimo e 15 anos [52, 53].

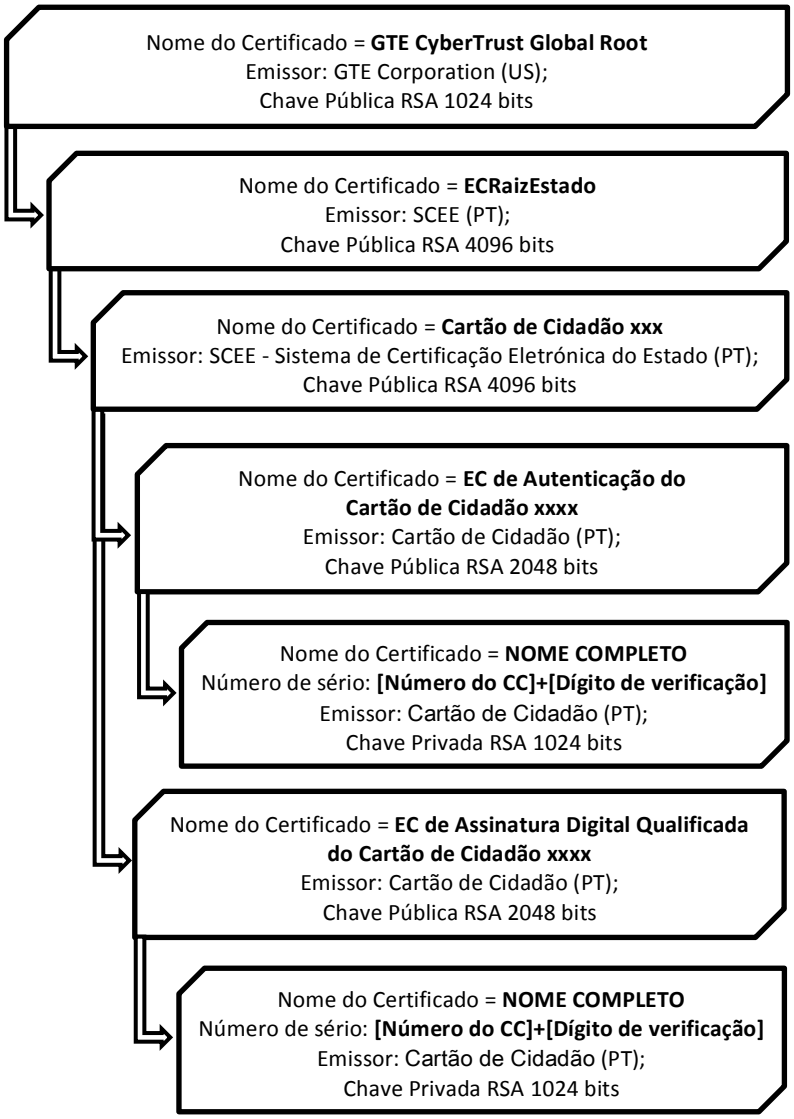

Nome do Certificado = **GTE CyberTrust Global Root**
Emissor: GTE Corporation (US);
Chave Pública RSA 1024 bits
Nome do Certificado = **ECRaizEstado**
Emissor: SCEE (PT);
Chave Pública RSA 4096 bits
Nome do Certificado = **Cartão de Cidadão xxx**
Emissor: SCEE - Sistema de Certificação Eletrónica do Estado (PT);
Chave Pública RSA 4096 bits
Nome do Certificado = **EC de Autenticação do Cartão de Cidadão xxxx**
Emissor: Cartão de Cidadão (PT);
Chave Pública RSA 2048 bits
Nome do Certificado = **NOME COMPLETO**
Número de sério: **[Número do CC]+[Dígito de verificação]**
Emissor: Cartão de Cidadão (PT);
Chave Privada RSA 1024 bits
Nome do Certificado = **EC de Assinatura Digital Qualificada do Cartão de Cidadão xxxx**
Emissor: Cartão de Cidadão (PT);
Chave Pública RSA 2048 bits
Nome do Certificado = **NOME COMPLETO**
Número de sério: **[Número do CC]+[Dígito de verificação]**
Emissor: Cartão de Cidadão (PT);
Chave Privada RSA 1024 bits

Figura 15: Esquema de certificação usado no cartão de cidadão

2.4.2 Cartão da ordem dos médicos

Recentemente a Ordem dos Médicos anunciou a criação de cartões de identificação profissional [14] com o objectivo de substituir e renovar as cédulas profissionais de forma a desenvolver uma solução de maior segurança para o médico em matérias como a PEM e meios complementares de diagnóstico, com incorporação de funcionalidades de Assinatura Digital Qualificada. [54]

Este cartão profissional, à semelhança do CC, consiste num documento que assume uma dupla funcionalidade:

- De documento físico, que permite a identificação visual e presencial do profissional
- De documento digital, que permite a identificação do profissional e autenticação eletrónica perante serviços digitais geridos por entidades públicas e privadas.

Tal como o cartão de cidadão, este contém "um conjunto de informações relativas ao médico impressas no cartão e um outro conjunto de informações contidas no chip eletrónico (todas as especialidades, subespecialidades, competências e dados relativos à autonomia do médico) e uma Assinatura Digital Qualificada equivalente à assinatura qualificada legal do Médico, tal como reconhecida pela ordem dos médicos, e associada ao nome completo, o nome clínico, número de cédula, a especialidade do médico (se tiver mais do que uma terá que decidir qual pretende incluir) e um endereço de email". [54]

A sua principal vantagem reflete-se na capacidade de aplicar criptografia de chave pública-chave privada (criptografia assimétrica), e dispor de sectores de armazenamento de dados protegidos por um código de

identificação pessoal (PIN), que permitem o armazenamento de uma chave de acesso pessoal (criptografia simétrica) e de senhas de uso único (one-time pad).

A OM, como entidade reguladora dos profissionais médicos, passa a assumir o papel de uma CA com a responsabilidade de criar, armazenar e gerir as identidades digitais dos profissionais com autorização para exercer medicina em território nacional, através dos serviços de uma PKI. A propagação das chaves públicas às várias entidades e instituições da área da saúde possibilita a verificação da elegibilidade do profissional em tempo real. Se um determinado profissional de saúde deixar de estar autorizado a prescrever, a sua chave pública é imediatamente revogada, ficando este automaticamente impedido de tomar decisões prescritivas nos sistemas electrónicos que validem os certificados na PKI da ordem dos médicos. Este vê-se assim obrigado a regularizar a situação perante a OM, para poder continuar a interagir com os sistemas de informação como profissional autorizado. A chave privada fica na posse dos médicos, devidamente protegida no chip do CPE, estando assim garantidas a segurança das credenciais dos mesmos.

A criação do cartão profissional eletrónico (CPE) teve início em Novembro de 2012 e apenas pode ser realizado com um contacto presencial do profissional médico nas secções regionais da Ordem dos Médicos. Após a confirmação da identidade e recolha dos dados necessários, estes são depositados junto da SIBS (entidade responsável pela personalização e gestão dos cartões bancários) e da Multicert (entidade responsável pela emissão dos Certificados Digitais Qualificados) através de um SFTP (secure file transfer protocolo) [54].

A entrega dos cartões está prevista que ocorra no decurso do ano de 2013, de acordo com o ciclo de produção dos mesmos.

Este processo permite não só atribuir os CPE mas também elaborar uma lista atualizada dos médicos que se encontram no ativo e produzir um directório com os seus certificados públicos. Desta forma, evita-se um problema antigo na área médica em que existiam médicos não credenciados ou autorizados a prescrever, que serviam de base a vários esquemas de fraude [17] em grande escala, extremamente lesivos dos interesses do estado e dos cidadãos.

Na secção relativa à proposta do SPE pretende-se usufruir das capacidades do CPE, nomeadamente dos certificados digitais inseridos no mesmo de forma a autenticar os profissionais e a proporcionar o não repúdio das informações transaccionadas.

2.5 Pescrição Eletrónica de Medicamentos

Em termos mundiais, os dois maiores mercados de sistemas de prescrição são os Estados Unidos da América e a Europa.

De acordo com o relatório de estratégias para a e-Saúde (eHealth Strategies Report) [55], a PEM define-se como sendo a introdução e a transferência de prescrições, por via eletrónica, desde um profissional de saúde até a uma farmácia, de forma a permitir a entrega dos medicamentos e o registo da dispensa nos registos médicos do paciente.

O Guia de Prescrição Eletrónica da *American Medical Association* [56], define mais exaustivamente o conceito de Prescrição eletrónica (*Electronic prescribing* ou e-*prescribing* ou *e-Rx*),como consistindo no uso de um computador ou qualquer outro dispositivo associado a componentes de *hardware* ou software que permite aos prescritores:

- Aceder a informação clínica eletrónica do paciente (histórico de medicações anteriores, sistemas de saúde associados e reações medicamentosas registadas) com o consentimento do paciente;
- Transmitir os dados da prescrição electronicamente;
- Permitir ao paciente aceder aos medicamentos prescritos em qualquer farmácia ligada ao sistema;
- Receber alertas eletrónicos relacionadas com a renovação da medicação crónica de um paciente quando esta se esgota;
- Suportar todo o processo de gestão medicamentosa – prescrição, transmissão, dispensa, administração e monitorização.

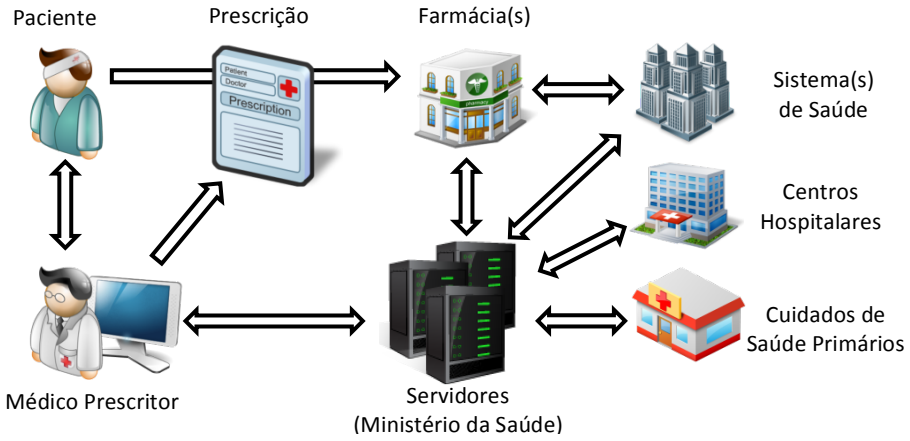


Figura 16: Esquema de um SPE

Para que tal seja possível, é necessário a implementação de um sistema de comunicação que interaja com os prescritores, os utentes e os sistemas de saúde associados, e as farmácias (Figura 16).

Desta forma, um SPE qualificado terá que ser capaz de [56]:

- Gerar uma lista de medicação ativa;
- Selecionar, imprimir e transmitir electronicamente as prescrições mantendo todos os níveis de segurança necessários para cada um dos processos;
- Integrar sistemas de apoio à decisão clínica (com aviso de possíveis reações adversas, alergias, interações medicamentosas, medicação ou doses não apropriadas)
- Proporcionar informações relacionadas à disponibilidade dos medicamentos existentes e respectivo preço, alternativas às mesmas, com capacidade de escolha das terapêuticas com menos custo financeiro;

- Disponibilizar informações sobre elegibilidade do paciente para medicações de prescrição especial e os sistemas de saúde em que este se encontra associado;
- Rever a medicação atual do paciente, o histórico medicamentoso e a dispensa medicamentosa das prescrições anteriores durante a consulta médica podendo atualizar a terapêutica em vigor perante o consentimento do paciente;
- Integrar sistemas de informação que informem o histórico do paciente e a situação clínica atual.
-

2.5.1 Publicações sobre a Segurança na PEM

Usando os os termos MESH relativos a "Software" e "Electronic Prescription", foram encontrados 46 artigos possíveis, dos quais selecionados seis artigos sobre os sistemas de precrição eletrónica implementados noutros países. Foi ainda feita revisão bibliográfica e pesquisa na Google® onde se encontraram outros documentos não indexados.

No contexto global da proteção de informações clínicas, a privacidade de dados das prescrições merece um destaque especial. Em primeiro lugar, a quantidade de entidades não médicas envolvidas torna qualquer sistema de prescrição complexo e de difícil gestão. Em segundo, a participação dos prescritores e dos utentes deve ser protegida, nomeadamente a identidade e confidencialidade das informações transaccionadas. Por outro lado, o processamento da prescrição não deve ser realizado de forma completamente anónima uma vez que é necessário identificar os intervenientes em determinadas situações (por exemplo intervenção legal) pelo que os dados devem circular anonimizados mas sempre com a possibilidade de serem associados, a nível central (neste caso ao nível do Ministério da Saúde), às entidades correspondentes, de forma a permitir processos de investigação e apurar responsabilidades. [37]

São raros os sistemas de prescrição corretamente implementados [57] e a fragmentação da informação em vários sistemas e organizações exige uma preocupação adicional relativamente à segurança com que os dados clínicos são transmitidos. A segurança dos dados é facilmente negligenciada nas Entidades de Saúde Públicas uma vez que esta não tem um impacto direto relacionado com a gestão ou com as finanças das organizações. O

manuseamento incorreto destas informações pode resultar em danos catastróficos para os indivíduos envolvidos relacionados com seguradoras privadas, empresas de crédito e mesmo a níveis profissionais. [57]

A ideia de utilizar *smartcards* com capacidades de identificação digital aparece descrita na literatura desde 1997 por Jaakko Niinima e Jari Forsstro (especialistas em Informática Médica na Finlândia) [57, 58] com referências a estudos piloto do *TROPPI-project* (Figura 17). O conceito de prescrição eletrónica é também para eles uma mais-valia relativamente à gestão medicamentosa e financeira. As terapêuticas medicamentosas atribuídas em meios extra-hospitalares acabam por ser as mais problemáticas relativamente à prescrição de fármacos diferentes, semelhantes ou iguais tornando por vezes os pacientes polimedicados. No entanto é curioso reparar na brevidade com que se afirmam que "a integridade, a segurança e a confidencialidade dos dados devem estar asseguradas". [58] Neste caso foi previsto um sistema com autenticação quer dos profissionais, quer dos utentes, sendo ambos detentores de um *smartcard* com capacidade de autenticação e assinatura digital (através da introdução de um código PIN), com acordo mútuo entre ambos os intervenientes e com possibilidade de delegar o responsável pela prescrição.

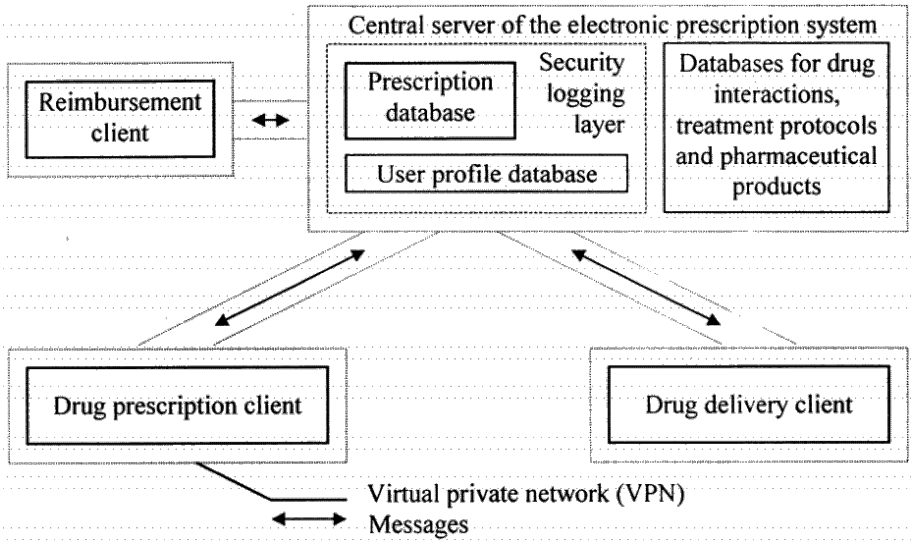


Figura 17: Esquema representativo do *TROPPI-project* [58]

Os autores deste projeto concluíram que o uso de *smartcards* parece ser o método de encriptação e de autenticação com mais facilidade de implementação, fazendo referência a um possível método de pseudo-anonimização da identidade dos intervenientes para minimizar os problemas de segurança e confidencialidade dos dados envolvidos. [58, 59]

No Reino Unido verifica-se uma preocupação com os dados clínicos existentes nas prescrições eletrónicas mesmo antes da implementação do SPE. Em termos de literatura, encontra-se a publicação de questionários com o intuito de perceber o ponto de vista dos médicos, farmacêuticos e pacientes relativamente à prescrição eletrónica [60] e um artigo descritivo de possíveis falhas de segurança (relacionadas com confidencialidade dos dados, autorização de acesso, identificação dos indivíduos, autenticação no sistema, auditoria, etc.) que poderão representar barreiras na implementação do mesmo. [61]

Nos Estados Unidos da América (após uma análise dos softwares de prescrição existentes realizada em 2005, através de inquéritos dirigidos a várias classes profissionais relativamente às funcionalidades dos SPE) verificou-se que um dos pontos mais enfatizados correspondia aos níveis de segurança e à confidencialidade dos dados. [62]

Mais recentemente (Setembro de 2012) foi ainda publicado um artigo pelo Departamento de Ciência de Computadores e Engenharia da National Chung Hsing University na Tailândia, onde foi proposto um SPE semelhante ao proposto neste trabalho. [63] Este estudo apresenta a proposta de um sistema de informação médico integrado numa arquitetura orientada para a distribuição de serviços informáticos (SOA - Service-Oriented Architecture) de maneira a facilitar a comunicação entre os vários sistemas de informação. A defesa do anonimato dos intervenientes (através do uso de pseudónimos nos pacientes e médicos envolvidos), o uso de assinaturas de grupo (*proxy signatures*) e ao mesmo tempo controle sobre as prescrições realizadas e disponibilizadas pelas farmácias de forma a evitar vários cenários de corrupção torna este artigo interessante de ser analisado.

2.5.2 Prescrição Eletrónica na Europa

A PEM foi implementada nos 27 países membros da Europa durante as últimas décadas. Foram muitos os projetos-pilotos lançados e vários os sistemas implementados.

Patrick Kierkegaard realizou recentemente um estudo relativamente à prescrição eletrónica na Europa onde verificou uma heterogeneidade de políticas, legislações e critérios de privacidade relativamente a proteção de dados, protocolos de transmissão de dados e esquemas de assinatura digital. Concluiu que nem todos os países apresentam infraestruturas capazes de suportar os sistemas, principalmente pelos custos elevados inerentes e pelos níveis de segurança não satisfatórios. [64]

Os sistemas de saúde variam entre si relativamente às comparticipações aplicadas aos tratamentos, financiamentos, taxas aplicadas aos utentes e custos diretos para o estado, sendo por exemplo o sistema Holandês considerado um sistema de saúde de referência mundial. [65]

A verdadeira PEM engloba três fases: a emissão da prescrição (eCapture), a transferência dos dados (eTransfer) e a dispensa dos medicamentos (eDispense). Embora haja uma aposta cada vez mais forte na implementação de um verdadeiro SPE, eram poucos os países que tinham implementado os vários sistemas, em 2010 (Tabela II). [55] Apenas a Dinamarca e a Suécia parecem ter realmente adotado um SPE a nível nacional de acordo com o conceito descrito. [66]

Tabela II: Estado da Prescrição Eletrónica na Europa em 2010

	eCapture	eTransfer	eDispense
Sistemas existentes	15	9	7
Sistemas Projetados	5	8	6
Sem sistemas	12	15	19

Adaptado de eHealth Strategies Report, 2011 [55]

Os valores da tabela anterior são concordantes com informações publicadas noutros relatórios [67-69], relativamente à implosão do mercado de sistemas de prescrição na Europa, prevendo que o número de sistemas vendidos triplicará entre 2011 e 2017, atingindo um investimento de mais de 500 milhões de euros de euros.

Um estudo multicêntrico realizado na Europa entre 2002 e 2011 concluiu que, ao contrário do que se imagina, apenas cinco nações apresentavam a PEM como prática diária. [66] Curiosamente dezasseis países incluíram a PEM como um objectivo nos planos de estratégia para a saúde nacional, mas poucos foram os que verdadeiramente implementaram uma rede de PEM completamente funcional, nos quais se incluem a Dinamarca, Suécia, Islândia e Estónia.

Nos países escandinavos (nomeadamente Dinamarca, Suécia e Holanda) verifica-se uma adopção intensa dos SPE, o que se justifica pelo investimento precoce nesta área da informática médica.

A Dinamarca inaugurou o seu SPE há mais de 10 anos e apresenta atualmente um sistema de prescrição e dispensa eletrónica que, para além de armazenar as prescrições de forma segura, permite o acesso das mesmas por parte dos pacientes, dos seus médicos prescritores e dos

farmacêuticos, a partir de um portal do ministério da saúde (apoteket.dk). Em 2011, cerca de 85% das prescrições foram enviadas electronicamente. [70]

A história da PEM sueca já é mais antiga, com início em 1981, igualmente com um sistema de prescrição e dispensa eletrónica. Neste caso há referências ao uso de cartões de identificação eletrónicos que permite associar e autenticar os pacientes durante o ato de dispensa. De igual forma foi implementada uma plataforma para consulta das prescrições anteriores (apoteket.se) que pode ser acedida pelo paciente e, apenas com consentimento do próprio, pelo médico e pelo farmacêutico de forma a otimizar as terapêuticas. Em 2012, foram prescritas cerca de 70.000 receitas por dia. [71, 72]

Primeira rede holandesa ligada à saúde foi implementada em 2002, e serviu de base para a criação de uma infraestrutura tecnológica que permitia a comunicação médico-médico e médico doente (de acordo com os níveis de segurança exigidos). A transição para um SPE completo iniciou-se em 2012, sob o abrigo de uma lei que obrigava a transmissão das PEM via eletrónica. Atualmente a Holanda apresenta um SPE e dispensa eletrónica, que processa cerca de 75% das receitas prescritas. [60, 73]

A Estónia, embora só tenha implementado um verdadeiro SPE em 2010, em apenas 15 meses consegui desmaterializar com sucesso (85% das receitas são por via eletrónica) todo o processo de prescrição [27], tal como

os países anteriores, tendo sido galardoada com vários prémios e representado a Estónia no World Summit Award 2011*.

Vários países encontram-se ainda no processo de desmaterialização das prescrições com o objectivo de consolidar o SPE, associado a projetos-piloto, tais como Áustria, Bélgica, Bulgária, Croácia, Chipre, República Checa, Inglaterra, Finlândia, França, Alemanha, Grécia, Hungria, Itália, Letónia, Irlanda do Norte, Noruega, Polónia, Portugal, Roménia, Eslováquia e Espanha. Os restantes países (Irlanda, Malta, Luxemburgo, Lituânia) não apresentam infraestruturas ou projetos relacionados com a prescrição eletrónica. [64] No caso da Finlândia e da Noruega, já existe legislação que prevê a obrigatoriedade de uso dos SPE com dispensa eletrónica ainda em 2013, o que os coloca no segundo patamar de evolução da PEM.

Os principais entraves à implementação dos sistemas relacionam-se com questões de complexidade do sistema, dificuldade em interligar o sistema de saúde com os serviços sociais, não adesão por parte dos médico e/ou farmacêuticos, ou por falta de confiança ou de informação por parte dos utentes.

Portugal, embora se tenha aventurado na PEM desde 2004, em 2010 apresenta uma percentagem considerável de receitas manuscritas, uma vez que apenas 64% das prescrições, em 2010. [55] Neste momento sabe-se que esse número sofreu um forte incremento, principalmente com a publicação de legislação que obriga a prescrição eletrónica. [10]

* http://www.wsis-award.org/

Relativamente aos SPE, o uso de smartcards na área da saúde apresenta vários tipos de aplicações, que podem assumir um papel de:

- cartão de identificação digital;
- dispositivo de armazenamento da informações médicas mais relevantes;
- dispositivo de autenticação do utente;
- dispositivo de autenticação do profissional de saúde.

Alguns países como a Suécia apresentam todas as estas capacidades implementadas. Em Portugal, o cartão de utente encontra-se incluído no cartão de cidadão (sobre a forma de um número), mas sem outro tipo de uso na área da saúde. [71]

2.5.3 Projeto epSOS

Na temática da PEM no estrangeiro, é importante referir um dos maiores projetos europeus atualmente em vigor: epSOS (Smart Open Services for European Patients).

Iniciado em 2008, este pretende projetar, criar e avaliar uma infraestrutura que permita a dispensa eletrónica multinacional através da interação entre múltiplos sistemas de informação médica e PEM. [74] Este sistema pretende usar os serviços de PEM entre os vários países aderentes e até ao final de 2013 prevê-se que seja implementado em 23 países europeus (Figura 18). [75]

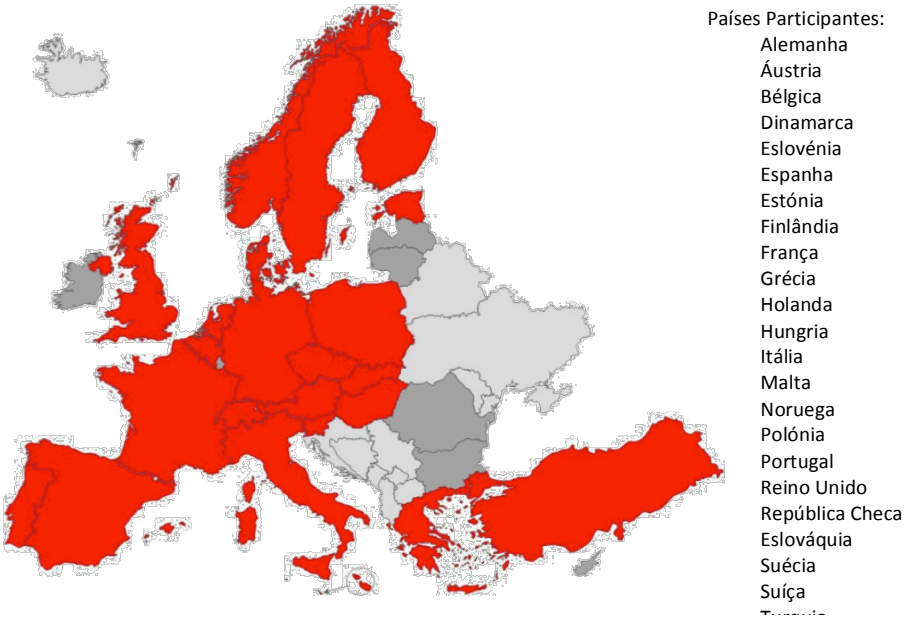


Figura 18: epSOS - Lista de países aderentes ao projeto

Fonte: www.epsos.eu

Neste momento existem dois projetos-piloto relacionados com a prescrição eletrónica e a dispensa eletrónica que decorrem na Áustria, Dinamarca, Espanha, Eslováquia, Finlândia, Grécia, Itália, Malta e Suécia (Figura 19).

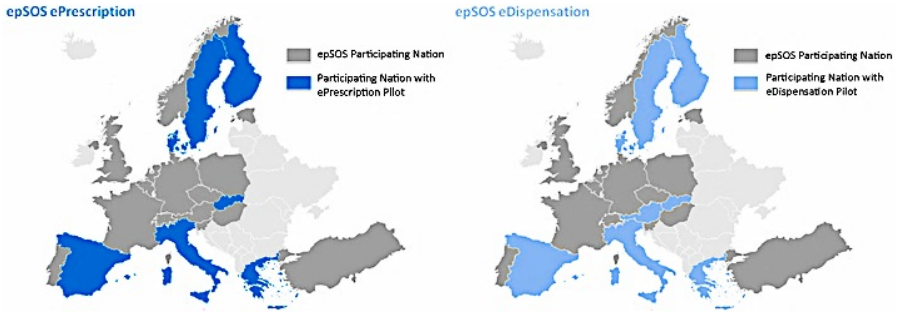


Figura 19: epSOS - Projeto-piloto de prescrição e de dispensa eletrónica

Fonte: www.epsos.eu

Estes sistemas usam os dados existentes nas prescrições eletrónicas e os dados de identificação dos pacientes. Os prescritores acedem ao sistema através de uma interface web onde se autenticam com as credenciais de acesso fornecidas pelo epSOS e as prescrições são processadas e armazenadas numa rede constituída pelos Pontos de Contacto Nacionais (NCP - National Contact Point) de cada país que comunicam entre si.

Posteriormente o paciente identifica-se numa farmácia e solicita os medicamentos que lhe foram prescritos. Durante a dispensa são registados os medicamentos solicitados e removidos da lista de medicação associada ao paciente. [74]

Este processo apenas se aplica aos profissionais prescritores e farmácias aderentes ao projeto e, em ambos os momentos (prescrição e dispensa), o paciente deve consentir o acesso às suas informações pessoais.

O conceito do epSOS é excelente mas apresenta algumas limitações inerentes à globalização de um sistema:

- não permite a comparticipação dos medicamentos por parte dos sistemas de saúde (quer para o utente, quer para a farmácia);
- não permite a prescrição de medicamentos de uso restrito;
- não existe uma comercialização global de todos os medicamentos, pelo que podem estar restritos à dispensa do país onde foram prescritos.

3 Sistema de Prescrição Atual

Nas páginas seguintes descrevemos o sistema de prescrição português com especial ênfase para as falhas de segurança existentes, baseado nas especificações técnicas para a elaboração de soluções de *software* nas instituições e serviços do Sistema de Saúde disponibilizado pela ACSS [76] e na experiência do ponto de vista to utente, médico e informático.

Este sistema encontra-se dividido em duas vias distintas: o SPE e o SPM (dependente de formulários específicos apenas permitido a título de exceção, de acordo com a legislação portuguesa [10]).

3.1 SPM - Sistema de Prescrição Manual

A prescrição manual é realizada através de impressos seriados (vulgarmente conhecidos como "receitas"), obtidos na Ordem dos Médicos (OM), preenchidas com a identificação do utente, número do Sistema Nacional de Saúde (ou outro subsistema) e com a descrição da medicação (máximo de 4 embalagens por receita) e respectivas posologias.

As receitas são validadas com uma vinheta do médico prescritor, uma vinheta do estabelecimento onde foram prescritas (caso se verifique) e com a assinatura do próprio (Figura 21).

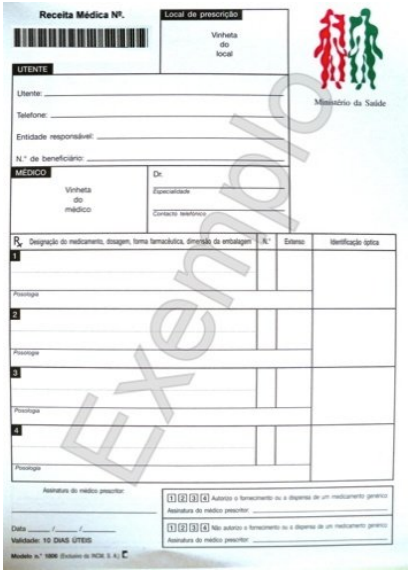


Figura 20: Receita Manual (2012)

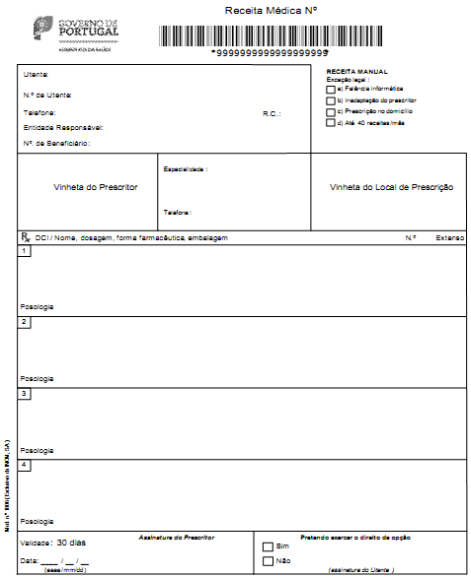


Figura 21: Receitas Manuais (2013)

Dada a legislação atual, o uso das receitas manuais só pode ser feito a título excepcional [77], sendo apenas admitidas receitas simples (1 via), caso haja falência do sistema informático, inadaptação fundamentada do prescritor (previamente confirmada e validada anualmente pela respectiva

Ordem profissional), prescrição ao domicílio ou outras situações (até um máximo de 40 receitas médicas por mês).

Os impressos ainda em vigor (Figura 20) serão atualizados a partir do dia 1 de Abril de 2013 [78] assumindo a forma retratada na Figura 21.

No dia 1 Dezembro de 2012 iniciou-se a produção de um novo modelo de vinhetas [79], que diferem das anteriormente utilizadas por apresentarem uma Imagem holográfica de 8 mm no canto superior direito da vinheta, com o logótipo do Ministério Saúde, em película metálica prateada e com numeração não seriada a partir de um código alfanumérico único por vinheta e correspondente ao código de barras, podendo ou não estar descrito o local de prescrição do profissional de saúde (Figura 22). A identificação das folhas de vinhetas possibilita a revogação das mesmas em caso de perda / roubo. Está previsto o uso obrigatório destas novas vinhetas a partir de 15 de Fevereiro de 2013 [79].

Figura 22: Exemplo das Vinhetas em vigor a partir de 2013 (Pantone 305 U)

A receita manuscrita é entregue ao utente, que assume a responsabilidade de se dirigir a uma farmácia onde é realizada a dispensa do medicamento (Figura 23). Nesse momento, são registados os medicamentos descritos na prescrição e o nível de comparticipação por

parte do estado que posteriormente são encaminhados para o Centro de Conferência de Facturas do SNS (CCF). As funções da CCF consistem em assegurar a recepção dos ficheiros e documentos de prescrição, identificar falhas ou mesmo fraudes, contribuir para a racionalização dos recursos do SNS e apurar os valores em dívida para com os prestadores de cuidados de saúde. [11]

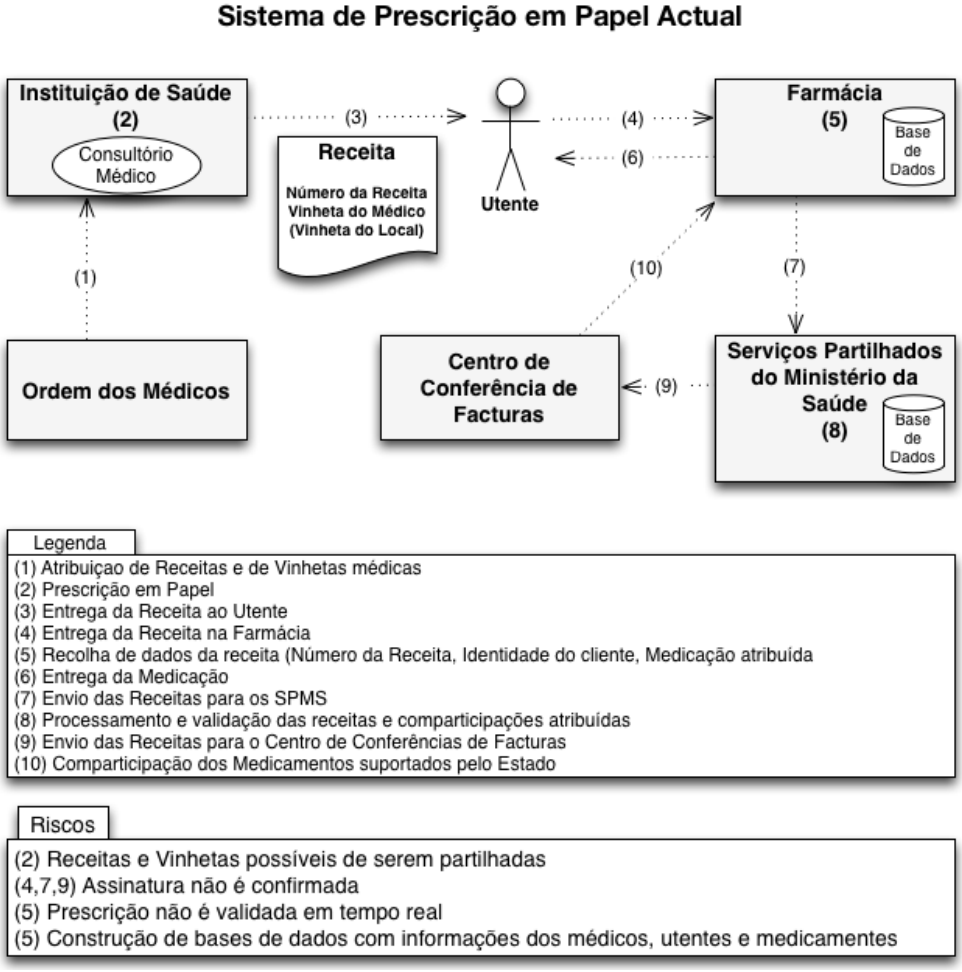

Sistema de Prescrição em Papel Actual
Instituição de Saúde
(2)
Consultório Médico
(3)
Receita
Número da Receita
Vinheta do Médico
(Vinheta do Local)
Utente
(4)
(6)
Farmácia
(5)
Base de Dados
(1)
(10)
(7)
Ordem dos Médicos
Centro de Conferência de Facturas
(9)
Serviços Partilhados do Ministério da Saúde
(8)
Base de Dados
Legenda
(1) Atribuiçao de Receitas e de Vinhetas médicas
(2) Prescrição em Papel
(3) Entrega da Receita ao Utente
(4) Entrega da Receita na Farmácia
(5) Recolha de dados da receita (Número da Receita, Identidade do cliente, Medicação atribuída
(6) Entrega da Medicação
(7) Envio das Receitas para os SPMS
(8) Processamento e validação das receitas e comparticipações atribuídas
(9) Envio das Receitas para o Centro de Conferências de Facturas
(10) Comparticipação dos Medicamentos suportados pelo Estado
Riscos
(2) Receitas e Vinhetas possíveis de serem partilhadas
(4,7,9) Assinatura não é confirmada
(5) Prescrição não é validada em tempo real
(5) Construção de bases de dados com informações dos médicos, utentes e medicamentes

Figura 23: Esquema do Atual Sistema de Prescrição Manual

Antes da criação do novo modelo de vinhetas, o nível de segurança das mesmas era baixo, uma vez que estas podiam ser facilmente replicadas. Atualmente, a atribuição de números não seriados às mesmas dificulta este tipo de fraude e possibilita a revogação se o proprietário comunicar à ordem profissional o seu extravio.

Neste processo é possível apontar várias falhas que potenciam usos indevidos ou fraudulentos na prescrição manual:

- A partilha de vinhetas do médico com terceiros;
- A entrega da receita nas farmácias que carece de uma validação em tempo real (a comunicação com a CCF é realizada posteriormente o que não permite confirmar a autenticidade do documento recebido ou da assinatura do prescritor no momento da dispensa).

A primeira falha depende da responsabilidade do prescritor, pelo que é importante alertar e responsabilizar o mesmo pelas vinhetas que lhe são atribuídas. A comunicação assíncrona com a CCF poderá ser complementada com uma notificação gratuita (via internet ou serviços de comunicação móvel) por parte do prescritor da prescrição realizada aos SPMS. Este sistema de notificação de uso dos impressos e vinhetas nas prescrições manuais, aumenta os níveis de segurança da prescrição e fomenta a prescrição eletrónica, mas pode representar um obstáculo para a prática clínica.

3.2 SPE - Sistema de Prescrição Eletrónica

O processo de prescrição eletrónica foi iniciado em 2004, tendo começado como um projeto-piloto em Portalegre, que foi alargado a nível nacional, dedicado às instituições associadas ao Sistema Nacional de Saúde (SNS) [2, 80]. Quando inserido no interior da Rede de Informação de Saúde (RIS), o sistema revelou-se estável e consistente, com níveis de segurança aceitáveis para um período inicial de implementação (Figura 24).

O ponto de instabilidade surgiu no momento em que o sistema de prescrição eletrónica foi alargado às entidades privadas que, por não se encontrarem incluídas na RIS, tornou necessária a criação de ligações entre estas e os SPMS.

A solução revelava potencial e, ao assumir um papel concêntrico de recepção das prescrições eletrónicas, permitiu um processamento mais eficiente. Todavia foram desvalorizados aspectos de segurança capazes de fragilizar um sistema promissor e com capacidades de vigorar no atual mundo da informática médica (Figura 24). A partir desse momento, foi delegada a função de transporte dos dados referentes às prescrições a empresas de *software* de prescrição, existindo uma lista de produtos certificados pelo ministério da saúde. [11] Inicialmente o *software* de prescrição estava sujeito a um processo de certificação essencial neste processo de desmaterialização da prescrição, contudo logo na fase inicial esta certificação foi substituída por uma declaração de conformidade do respectivo fornecedor junto dos SPMS [16, 77]. Note-se que esta "simplificação" do processo aumentou de forma significativa o risco de segurança por não existirem garantias reais da conformidade do *software* com a especificação técnica imposta.

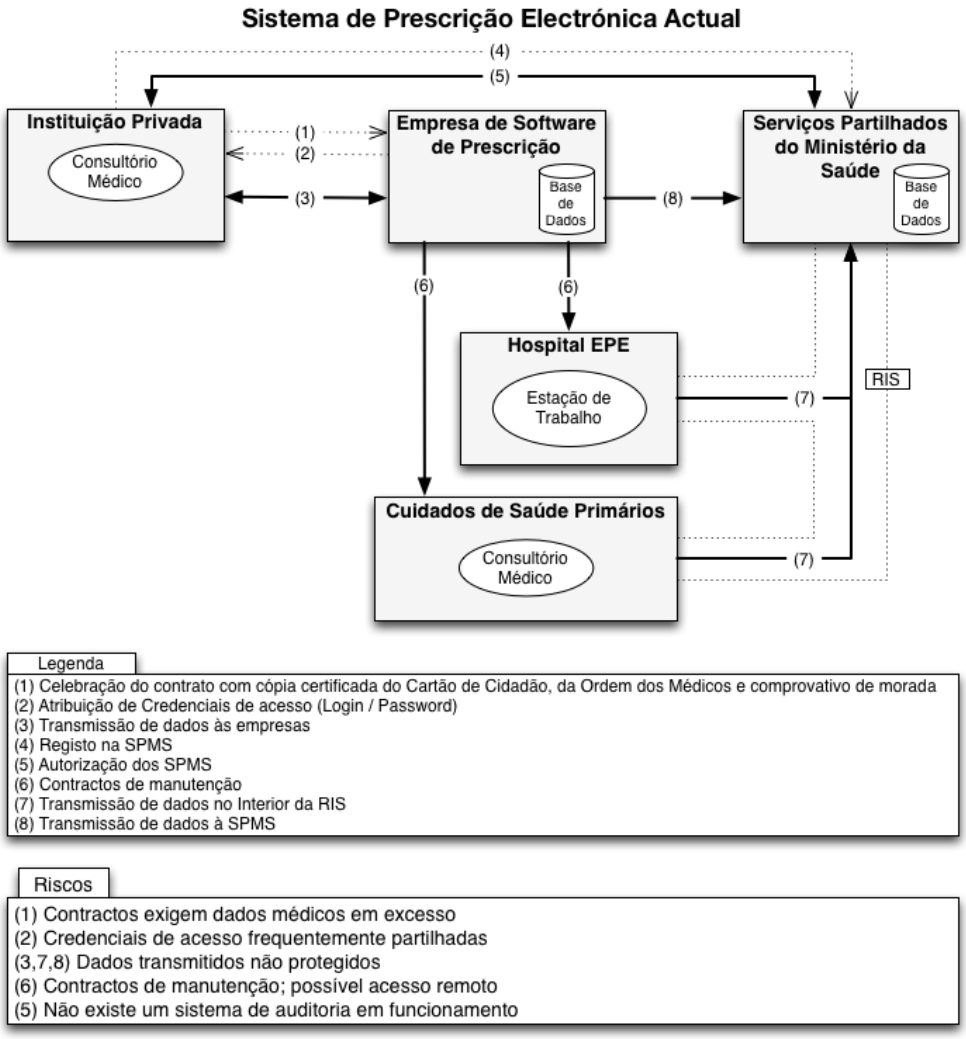


Figura 24: Esquema do Atual Sistema de Prescrição Eletrónica

Deveria ser possível, através de mecanismos de certificação digital, garantir que o *software* que está a ser usado não foi alterado e, ainda mais importante, garantir um sistema de auditoria eficiente de forma a certificar os softwares autorizados pelos SPMS.

Pouco tempo após da publicação do decreto, que definiu a PEM como obrigatória [10] e das condições de auditoria a que as empresas de PEM seriam submetidas, foi anunciada a possibilidade de iniciar este processo de formalização com o preenchimento de uma Declaração de Conformidade do Fabricante. [20] Recentemente, foi ainda publicitado pelos SPMS uma revisão das autorizações concedidas às empresas de software em que, só a partir de 1 de Abril de 2013, será criada uma lista de programas autorizados e uma lista dos programas não autorizados. [77] Infelizmente, parece ser novamente subvalorizada a necessidade de realização de auditorias nas instalações das empresas, sendo apenas requerido o preenchimento de uma declaração de auto-conformidade por parte das empresas*. Sem que seja posta em dúvida a honestidade ou responsabilidade das empresas, parece mais que justificável o envolvimento dos SPMS nestas autorizações dado o manuseamento de informações privadas e confidenciais dos vários intervenientes no sistema de prescrição.

O ano de 2011 ficou marcado por uma corrida dos profissionais prescritores em estabelecimentos privados, em busca de uma solução informatizada que permitisse o cumprimento dos novos decretos, onde foi possível assistir à inscrição de milhares de médicos nos sistemas de prescrição eletrónica.

A inscrição obriga, quase na maioria das companhias, ao preenchimento de um formulário padrão acompanhado de fotocópias autenticadas do cartão de cidadão (ou bilhete de identidade e cartão de contribuinte) e do cartão da OM, comprovativo de morada, contactos e de uma declaração onde o profissional "assume totalmente a responsabilidade por qualquer

* http://www.spms.pt/2012/12/declaracao-de-auto-conformidade

utilização indevida e/ou ilegal da mesma ilibando desta forma a [empresa de software] em qualquer litígio que lhe seja associado por este facto".

Os contractos celebrados parecem exigir demasiadas informações pessoais, irrelevantes para a inscrição num sistema de prescrição que, se usadas ilegalmente, possibilitam que uma outra pessoa possa prescrever em nome de médico contratado. Depois de realizado o contracto com as empresas de *software*, são atribuídas as credenciais de acesso à respectiva plataforma de prescrição.

Quanto à localização dos recursos informáticos, levanta-se a dúvida se estes se encontram em território nacional, uma vez que esta condição não está explícita na regulamentação e certificação das empresas os critérios referentes à localização dos servidores ou de possíveis *gateways* e servidores de backup. Fica também na dúvida se existe subcontratação de serviços de alojamento, algo que apenas é possível negar após realização de auditorias às várias empresas.

Por lei, o responsável pela contratação dos serviços de prescrição deve comunicar a contratação de serviços e o acesso a dados clínicos e proceder ao registo na base de dados de utentes na CNPD. [26, 81] Várias companhias publicitam esta informação mas nem sempre a mesma é mencionada.

A ligação é sempre estabelecida através da internet (requisito obrigatório para prescrever electronicamente), geralmente sob a forma de uma ligação segura (https ou TLS) entre os vários intervenientes, o que não garante proteção dos dados, pois não existe nenhum processo de cifra associado. Desta forma, durante o percurso da informação esta pode e é armazenada em bases de dados locais, antes de ser encaminhada para os

SPMS. Neste contexto, o facto de serem usados protocolos de transmissão de dados seguros pode dar um aspecto de segurança mas não invalida que o acesso ao sistema seja realizado pelo mesmo. Esta questão supõe o uso indevido das credenciais de acesso de um médico prescritor que permitam a prescrição em nome do mesmo ou acesso às prescrições do mesmo ou de outros profissionais, motivo pelo qual se impõe a necessidade de atribuição de credenciais de acesso por parte de uma entidade independente das empresas.

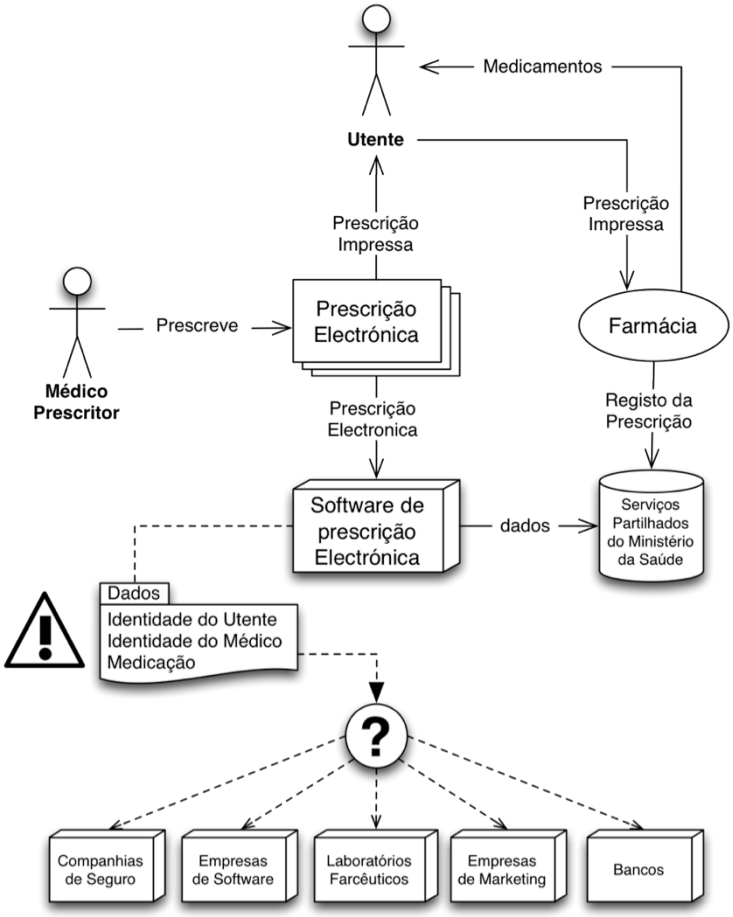


Figura 25: SPE, seus intervenientes e o potencial fuga de informação

Caso se verifique uma fuga de dados por parte das empresas de *software*, essa informação pode revelar-se valiosa para muitas organizações, desde laboratórios farmacêuticos (com interesses na área dos medicamentos) até companhias de seguros, instituições bancárias, ou mesmo para empresas que pretendem recrutar novos funcionários (com interesse na área da prescrição que permitisse inferir a situação clínica do indivíduo), como está exemplificado na Figura 25.

O sistema de prescrição eletrónica, anteriormente concebido para o SNS, dava uma sensação de segurança relativamente à transmissão de dados entre as várias instituições e a ACSS por operar no interior de uma rede de dados dedicada (RIS) e, teoricamente, isolada do exterior. Com a abertura para o mercado empresarial, começaram a surgir as Entidades Públicas Empresariais (EPE) e as instituições de saúde com modelos de gestão empresarial. Este passo fez com que a aquisição e uso de *software* de prescrição não fosse limitada ao software disponibilizado pelo ministério da saúde e pudessem ser escolhidos novas plataformas pelos diretores e gestores desses estabelecimentos. Com o aumento desta procura, também a oferta de serviços concorrentes começou a prosperar, de forma não controlada, existindo neste momento instituições ligadas à RIS e que contrataram os serviços de prescrição não-estatal. A união destas duas zonas gera dificuldades na gestão da segurança dos dados clínicos.

Algo que parece uma simples evolução do mercado de serviços na área da saúde pode, de facto, tornar-se uma potencial falha num sistema delicadamente instituído: a partir do momento que temos consciência dos dados que as empresas de *software* detêm (que mais uma vez, são informações pessoais e profissionais exigidas aquando a celebração de contractos com os médicos), e da área de ação que atualmente estas detêm

(fornecimento de serviços e manutenção informática no interior de entidades públicas), é possível quebrar a barreira isoladora de ambos os meios: a Rede de comunicação do SNS (RIS) e a Internet (onde permanecem a entidades de saúde privadas).

Existe um número considerável de médicos a exercer funções clínicas simultaneamente em instituições públicas e privadas, o que pode tornar cada vez exequível a prescrição dolosa com recurso à RIS. É possível, dentro de uma instituição pública, com recurso às informações/credenciais partilhadas entre múltiplos sistemas, prescrever em nome de um médico, uma vez que nestas o acesso à RIS é direto e não rastreável. Todo este quadro de hipotética usurpação de identidade e prescrição fraudulenta torna-se cada vez mais fácil e exequível com o avançar do tempo, se não forem tomadas as medidas corretas e necessárias.

Simultaneamente com a transmissão das informações para o servidor da empresa de *software* (e seguidamente para os SPMS) é impresso um documento com validade equivalente a uma prescrição em papel (Figura 26 e Figura 27). Este baseia-se num *template* disponibilizado pela ACSS que é entregue ao utente para comprovar perante o farmacêutico a comparticipação dos seus medicamentos.

A este cenário acrescenta-se ainda o desenvolvimento da Plataforma da Dados da Saúde (PDS) pela SPMS, que permite o acesso às informações clínicas dos utentes por parte dos médicos e por parte do próprio utente. A fragilidade descrita anteriormente para a prescrição eletrónica pode igualmente ocorrer nesta nova plataforma, uma vez que não estão completamente especificados os indivíduos e quais as condições (físicas,

hierárquicas, circunstanciais e temporais) em que se permite o acesso aos dados de saúde dos utentes. [76]

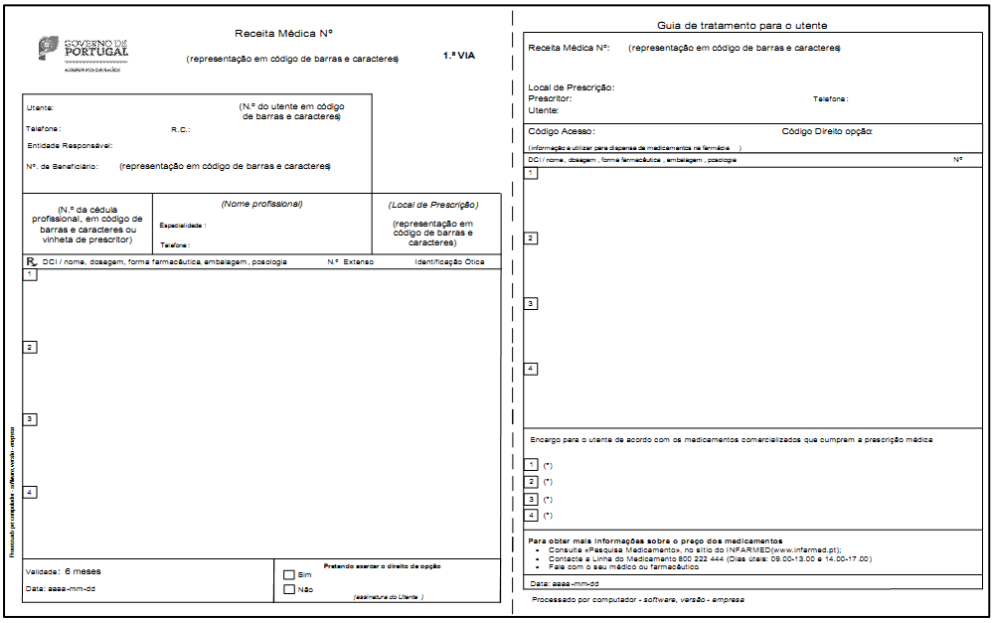

Receita Médica Nº
(representação em código de barras e caracteres)
1.ª VIA
Utente:
(Nº do utente em código de barras e caracteres)
Telefone:
R.C.:
Entidade Responsável:
Nº. de Beneficiário:
(representação em código de barras e caracteres)
(Nº da cédula profissional, em código de barras e caracteres ou vinheta de prescritor)
(Nome profissional)
Especialidade:
Telefone:
(Local de Prescrição)
(representação em código de barras e caracteres)
DCI / nome, dosagem, forma farmacêutica, embalagem, posologia
Nº Extenso
Identificação Ótica
Validade: 6 meses
Data: aaaa-mm-dd
Pretendo exercer o direito de opção
Sim
Não
(assinatura do Utente)
Guia de tratamento para o utente
Receita Médica Nº:
(representação em código de barras e caracteres)
Local de Prescrição:
Prescritor:
Telefone:
Utente:
Código Acesso:
Código Direito opção:
(informação a utilizar para dispensa de medicamentos na farmácia)
DCI / nome, dosagem, forma farmacêutica, embalagem, posologia
Nº
Encargo para o utente de acordo com os medicamentos comercializados que cumprem a prescrição médica
Para obter mais informações sobre o preço dos medicamentos
Consulte «Pesquisa Medicamento», no sítio do INFARMED(www.infarmed.pt);
Contacte a Linha do Medicamento 800 222 444 (Dias úteis: 09.00-13.00 e 14.00-17.00)
Fale com o seu médico ou farmacêutico
Data: aaaa-mm-dd
Processado por computador - software, versão - empresa

Figura 26: Esquema da PEM impressa em papel (frente)

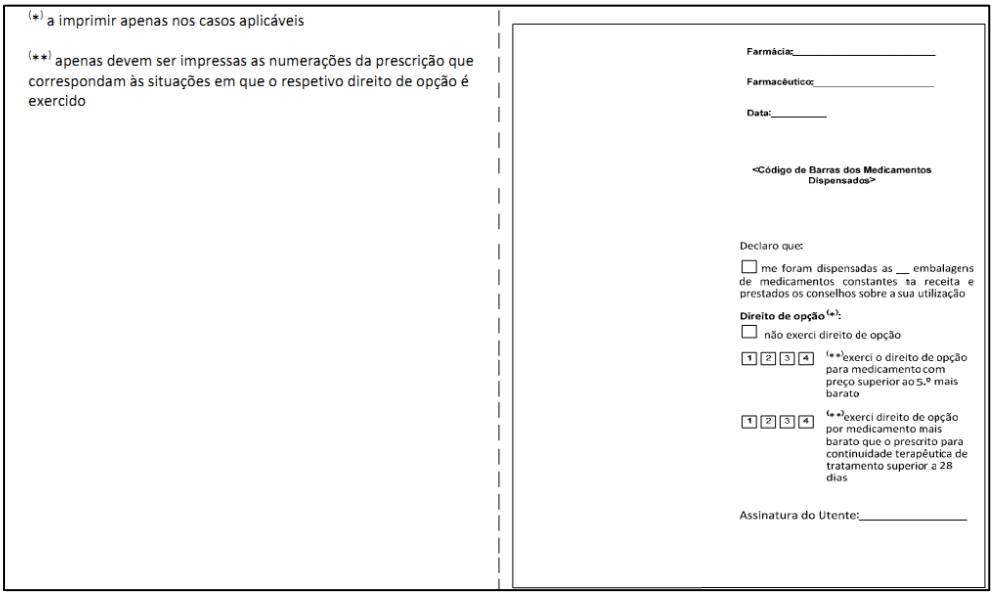

(*) a imprimir apenas nos casos aplicáveis
(**) apenas devem ser impressas as numerações da prescrição que correspondam às situações em que o respetivo direito de opção é exercido
Farmácia:
Farmacêutico:
Data:
<Código de Barras dos Medicamentos Dispensados>
Declaro que:
me foram dispensadas as __ embalagens de medicamentos constantes na receita e prestados os conselhos sobre a sua utilização
Direito de opção (*):
não exerci direito de opção
1 2 3 4 (**) exerci o direito de opção para medicamento com preço superior ao 5.º mais barato
1 2 3 4 (**) exerci direito de opção por medicamento mais barato que o prescrito para continuidade terapêutica de tratamento superior a 28 dias
Assinatura do Utente:

Figura 27: Esquema da PEM impressa em papel (verso)

Neste momento, o sistema de prescrição eletrónica apresenta várias fragilidades:

- Contractos exigem dados médicos que, potencialmente, permitem a prescrição em nome de outros (potencial usurpação de identidade digital)
- Credenciais de acesso partilhadas, o que permitem que outros prescrevam no nome do médico (potencial extorsão de identidade digital)
- Transferência de dados não encriptados entre o médico e a ACSS (perda de privacidade e possível roubo de informações clínicas)
- Receita com dados do utente (perda do direito à privacidade)

4 Avaliação da Percepção dos Riscos Segurança na PEM

4.1 Introdução

No ano de 2000 foi realizado um inquérito no Reino Unido de forma a perceber o ponto de vista dos médicos, farmacêuticos e pacientes relativamente à prescrição eletrónica. As preocupações mais referidas relacionavam-se com os níveis de segurança do sistema informático e possíveis problemas relacionados com a partilha de informações clínicas entre os médicos e as farmácias [82].

Nos últimos anos, tem-se verificado um aumento da preocupação por parte do público relativamente à potencial violação dos dados clínicos [83].

Francis France escreveu ainda alguns artigos sobre esta mesma temática, onde considera que a área da Saúde se encontra demasiado desprotegida e vulnerável a roubo de informação, corrupção da informação e acessos não autorizados [84]. Comparativamente com outros tipos de informação, os dados clínicos são de uma maior sensibilidade, quer pela necessidade de os mesmo estarem acessíveis a qualquer altura e durante um longo período de tempo [85].

Relativamente ao nível de consciência dos médicos prescritores relativamente aos níveis de segurança, não existe muita informação disponível na comunidade científica. Um questionário aplicado a cinquenta e seis médicos forenses no Reino Unido defende a necessidade de informação, educação e treino dos profissionais nesta temática [86].

É importante saber a opinião dos intervenientes do sistema, motivo pelo qual se realizou um inquérito, de forma a avaliar o nível de percepção dos riscos de segurança por parte dos utilizadores de *software* de prescrição, dos utentes e o funcionamento do SPE.

4.2 Métodos

Realizou-se um questionário anónimo, recorrendo à plataforma Medquest [23], constituído por 17 perguntas de resposta fechada, das quais quatro serviram para caracterização da amostra (Anexo 1). Simultaneamente foi programada uma ferramenta para aceder à página da Entidade Reguladora da Saúde (ERS) que tirou partido da sua estrutura sequencial, de forma a recolher os contactos dos responsáveis pelo sistema de prescrição eletrónico das várias clínicas privadas.

Foram enviados, por correio eletrónico, com um endereço único aleatorizado de forma a limitar o preenchimento do questionário a uma resposta por instituição. As respostas foram anónimas e não foram recolhidas informações pessoais sobre os profissionais que permitissem a

identificação dos mesmos. O inquérito iniciou-se no dia 24 de Janeiro de 2012 e esteve ativo até ao dia 22 de Fevereiro do mesmo ano.

Dos 9444 contactos de correio eletrónico iniciais, alguns endereços foram excluídos por diversas razões (endereço errado ou não uso de prescrição eletrónica), resumindo o universo da população a questionar a 7768 instituições. Alguns dos profissionais responsáveis pelo sistema de prescrição não são profissionais de saúde, pelo que apenas foram analisadas as respostas dos médicos. Todo o tratamento estatístico foi realizado com apoio no software SPSS®.

4.3 Caraterização da Amostra

Das 7768 instituições contatadas, apenas 836 respostas (11%) foram obtidas. Deste grupo de responsáveis pelo sistema de prescrição das entidades, 674 (81%) são médicos (amostra a ser estudada).

Da amostra em estudo, 465 (69%) são do sexo masculino e a média das idades é 52 anos.

A distribuição geográfica, como era previsível, aponta para um número de respostas mais elevado nas cidades com maior densidade populacional (Figura 28). Todavia as metrópoles de Lisboa e do Porto não exibem diferenças significativas nos valores totais

Todos os inquiridos apresentam um nível académico elevado, correspondente a 512 licenciaturas, 94 mestrados e 58 doutoramentos.

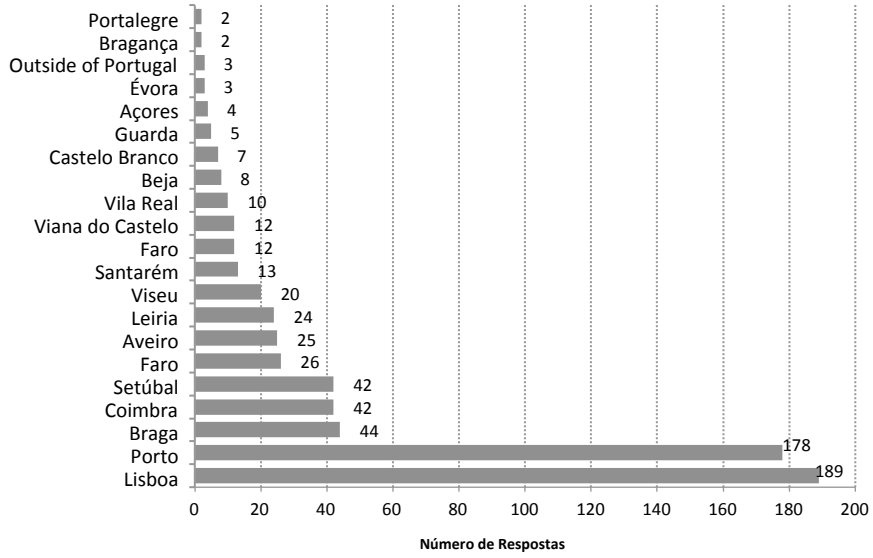


Figura 28: Distribuição geográfica da amostra populacional

4.4 Resultados

A Tabela III descreve o número de respostas obtidas nas questões sobre segurança e privacidade dos dados e a Tabela IV sumariza a média de Idades e o desvio padrão das respostas sobre segurança e privacidade dos dados. Os inquiridos que responderam não ter a certeza apresentam, em média, uma idade superior aos restantes.

Tabela III: Respostas às questões sobre segurança e privacidade dos dados

Pergunta	**Sim**		**Não**		**Não sei**	
	n	(%)	n	(%)	n	(%)
As suas credenciais de acesso (password) são conhecidas apenas por si?	538	(80)	82	(12)	54	(8)
Acha possível outra pessoa prescrever em seu nome?	142	(21)	336	(50)	196	(29)
Considera que, para a celebração do contrato com a empresa de prescrição eletrónica, cedeu demasiada informação pessoal?	203	(30)	373	(55)	98	(15)
Acha que a informação pessoal cedida, se comprometida, potencia a fraude usando a sua identidade digital?	357	(53)	139	(21)	178	(26)
Confia em empresas privadas para guardar os dados de prescrição médica dos seus pacientes?	348	(52)	326	(48)	—	—

Embora a maioria dos médicos (n=538) afirme que não partilha as suas credenciais de acesso, 232 (43%) não negam a possibilidade de outrem prescrever em nome dos mesmos.

Tabela IV: Média de Idades e Desvio padrão das respostas sobre segurança e privacidade dos dados

Pergunta	Sim		Não		Não Sei		p
	Méd	(dp)	Méd	(dp)	Méd	(dp)	
As suas credenciais de acesso (password) são conhecidas apenas por si?	52	(12)	51	(11)	53	(10)	0.578
Acha possível outra pessoa prescrever em seu nome?	51	(11)	52	(12)	52	(11)	0.681
Considera que, para a celebração do contrato com a empresa de prescrição eletrónica, cedeu demasiada informação pessoal?	50	(11)	52	(11)	54	(13)	**0.009**
Acha que a informação pessoal cedida, se comprometida, potencia a fraude usando a sua identidade digital?	50	(12)	53	(12)	54	(11)	**0.003**
Confia em empresas privadas para guardar os dados de prescrição médica dos seus pacientes?	51	(11)	53	(12)	-	-	**0.024**

Apenas 50% dos médicos inquiridos afirmam ter conhecimento que é dever dos profissionais clínicos informar os seus pacientes relativamente ao processamento e transmissão dos dados clínicos. A opinião dos restantes divide-se, sendo que 22% acreditam ser responsabilidade das companhias de software e 28% desvalorizam esta questão ao admitirem que os pacientes não precisam de receber essa informação.

Observe-se ainda que maioria (76%) considera as empresas de *software* como responsáveis pela notificação à CNPD; apenas 18% dos médicos inquiridos responderam corretamente ao assumir a responsabilidade dos mesmos e 5% consideram esta atitude como desnecessária.

Analisou-se a opinião dos médicos relativamente às possíveis entidades interessadas nos dados das prescrições (Figura 29) com recurso à média das pontuações para cada entidade numa escala de 1 a 4 ("sem interesse" a "altamente interessada").

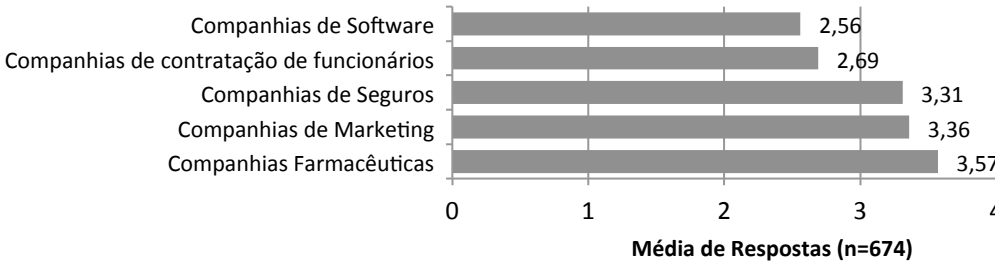


Figura 29: Respostas sobre as entidades interessadas nos dados das prescrições

Foram elaboradas perguntas de escolha múltipla para analisar as principais desvantagens da prescrição eletrónica do ponto de vista do médico (Figura 30) e a perceção que estes detêm relativamente à

localização dos dados clínicos nos sistemas de prescrição eletrónica (Figura 31).

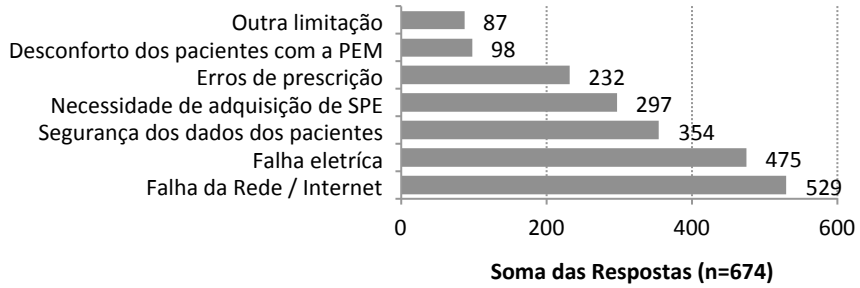


Figura 30: Respostas sobre as desvantagens da prescrição eletrónica

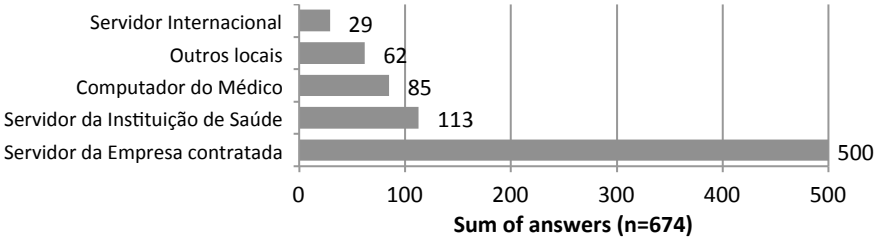


Figura 31: Respostas sobre o armazenamento dos dados das prescrições

4.5 Discussão dos Resultados

Uma vez que a prescrição eletrónica é obrigatória desde 2011 [10], é importante que haja transparência na informação e que os profissionais médicos e os utentes estejam cientes do sistema que atualmente se

encontra em vigor. Barrows dissertou sobre a partilha das credenciais de acesso aos sistemas hospitalares entre os vários médicos hospitalares, ação que revela uma falta de percepção dos riscos provocados por estas ações e pode ser justificada pela implementação ainda recente dos atuais sistemas de informação. [24] Verifica-se um esforço por parte dos responsáveis informáticos em solidificar a segurança dos sistemas médicos, sendo atribuídas credenciais de acesso mais seguras (combinações de letras e números), ainda que, em inúmeras situações, os profissionais acabem por anotar as palavras-chave nos teclados ou monitores dos terminais que usam frequentemente, ou substituem-nas por uma senha pessoal e de fácil memorização (e também facilmente descobertas).

Relativamente à partilha de palavras-chave, 20% dos clínicos admitiram partilhar as passwords ou não terem conhecimento se tal acontecia (Tabela III). Este valor é demasiado elevado uma vez que podem existir potenciais acessos aos sistemas de saúde, pondo em risco a privacidade, integridade e confidencialidade dos dados das instituições. Mesmo os médicos que negaram a partilha das suas credenciais, metade dos mesmos não negam a hipótese de outra pessoa poder prescrever no nome destes. Os restantes acreditam que com as suas credenciais os dados se encontram seguros, o que não é verdade.

Outro aspecto interessante, relaciona-se com a responsabilidade de informar o paciente sobre a transmissão das suas informações clínicas, através da internet até ao servidor da companhia de software de prescrição eletrónica. Para além de parecer um aspecto trivial, não está definida se a localização dos dados corresponde à morada física da empresa responsável, existindo a hipótese, num caso mais extremo, que as informações dos utentes possam ser armazenadas em servidores internacionais. Para além

de apenas 50% dos médicos ter conhecimento desta regra, os 28% que desvalorizam este consentimento informado é muito preocupante.

Para a celebração de contrato entre um médico (ou uma instituição de saúde) com uma empresa de software de PEM, são exigidos vários dados dos profissionais médicos, acompanhados de fotocópias autenticadas do cartão de cidadão, cartão da ordem dos médicos, comprovativo de morada, entre outros elementos. Se esta a informação for comprometida, existe um risco elevado de furto de identidade digital, uma vez que estão reunidas todas as informações pessoais que caracterizam o profissional nos sistemas de prescrição eletrónica. Teoricamente, para realizar uma prescrição, bastaria uma autorização da ordem dos médicos, pelo que são exigidas demasiadas informações aos médicos que contratam serviços das companhias de softwares de prescrição. Infelizmente, apenas metade da amostra está consciente da possibilidade de roubo de identidade (Tabela III).

Os médicos mais jovens parecem mais suspeitos relativamente a três aspetos (Tabela IV): celebração dos contratos com as empresas de software de prescrição; possibilidade de serem vítimas de roubo de identidade digital caso a informação dos mesmos seja comprometida; e localização dos dados de prescrição dos seus pacientes.

De acordo com a legislação, "o responsável pelo tratamento ou, se for caso disso, o seu representante deve notificar a CNPD antes da realização de um tratamento ou conjunto de tratamentos, total ou parcialmente autorizados, destinados à prossecução de uma ou mais finalidades interligadas" [26]. Como se observou nos resultados, apenas 18% dos médicos inquiridos estão conscientes que é da responsabilidade dos

mesmos de notificar a CNPD do uso de software de prescrição eletrónica para atividades privadas. Estes resultados promovem questões sobre a suspeita de falta de informação, que poderia ser alertada pela Ordem dos Médicos, pelo Ministério da Saúde ou pelas Empresas de software de prescrição. De acordo com os relatórios de atividades da CNPD [23, 87] tem-se verificado um acréscimo dos pedidos de "acesso a dados de saúde de terceiros", ainda que a maioria diga respeito a acessos às fichas clínicas de titulares de dados já falecidos, o que nos leva a deduzir que efetivamente o número de profissionais de saúde verdadeiramente preocupados com esta questão seja de facto reduzido.

Do ponto de vista dos médicos, as empresas farmacêuticas são consideradas as entidades que mais beneficiariam dos dessas informações (Figura 29). Uma hipótese deste resultado pode estar relacionada com a tendência para uma competição crescente entre os laboratórios: com esta informação seria teoricamente possível exercer uma maior pressão, quer nos profissionais médicos, quer nos utentes, sobre a escolha das marcas de fármacos prescritos. O mesmo raciocínio pode ser aplicado às empresas de marketing, posicionadas em segundo lugar, pois permitiria a prática de marketing direcionado. Ainda com um potencial interesse elevado, seguem-se as companhias de seguros: estas informações permitem a construção de perfis medicamentosos dos quais é possível inferir, com algum grau de confiança, várias patologias associadas, o que podem ser responsáveis por situações de discriminação negativa.

Relativamente às possíveis desvantagens da prescrição eletrónica (Figura 29), a quebra da ligação de Internet e a falha da corrente eléctrica foram apontadas como as principais desvantagens. Contudo estes motivos são previstos pela lei, sob a forma de exceções, sendo permitida a

prescrição não eletrónica [10]. A segurança dos dados dos utentes surge apenas em terceiro lugar, o que leva a crer na necessidade de divulgação desta problemática entre os profissionais de saúde.

Sobre o armazenamento dos dados das prescrições (Figura 31), apenas 74% dos médicos acredita que os dados clínicos se localizam nos servidores das companhias de *software* de prescrição. Uma vez que estas companhias oferecem a opção de consulta de prescrições anteriores, os dados estão obrigatoriamente armazenados nos servidores das empresas, o que revela que pelo menos 26% dos médicos inquiridos não se encontra consciencializado da localização dos dados clínicos. As restantes opções (que não podem ser negadas) revelam que apenas uma pequena percentagem dos profissionais se apercebe que os dados podem estar armazenados em lugares menos seguros (servidores internacionais). A subcontratação de serviços de armazenamento de dados é cada vez mais frequentes nas empresas e, sem um sistema de auditoria eficiente, não é possível ignorar esta possibilidade.

Uma das limitações deste estudo relaciona-se com o número de respostas obtidas. A baixa taxa de resposta (11%) pode ser justificada pela forma como este foi distribuído (correio eletrónico), ainda que fosse desejável uma maior taxa de resposta de forma a garantir que os resultados fossem representativos da população médica.

4.6 Conclusão

O questionário foi orientado aos médicos responsáveis por um sistema de prescrição eletrónico, e como tal mais informados da legislação e das condições em que este é realizado. Ainda que apresente uma baixa taxa de resposta, são espectáveis piores resultados na população global de médicos.

Os resultados mostram que os médicos portugueses não se encontram conscientes de todos os riscos existentes no atual sistema de prescrição eletrónica. Uma vez que este modelo é obrigatória, deveria existir uma maior transparência no processo como esta é realizada e os médicos e os paciente deveriam ser esclarecidos quanto à localização das suas informações.

No entanto é possível melhorar o sistema e corrigir as falhas de segurança de forma a torná-lo robusto e mais credível.

Desta forma, para melhorar a situação atual, é importante:

- Consciencializar os médicos prescritores dos riscos descritos;
- Assegurar o cumprimento das regras da CNPD;
- Reformular os contratos realizados com as empresas de software de prescrição;
- Encriptar a transmissão de dados entre as instituições prescritoras e o Ministério da Saúde;
- Certificar as empresas de software de prescrição de forma a assegurar a qualidade dos serviços prestados no Sistema Nacional de Saúde e organizar auditorias periódicas.

5 SPE Proposto – Modelo eletrónico

Como se verificou nos capítulos anteriores, o atual SPE apresenta uma lista considerável de falhas de segurança que podem comprometer a estabilidade do próprio sistema, os dados privados dos seus intervenientes e potenciar a fraude.

Uma vez que o SPE se encontra implementado e integrado com uma multiplicidade de sistemas de informação, a solução mais viável passará pela correção das falhas apontadas e pela implementação de protocolos de comunicação e de dispositivos tecnológicos.

Neste momento, existe a vantagem de parte dos recursos tecnológicos estarem a ser aplicados, nomeadamente as CPE, os leitores de smartcards e o aprovisionamento de certificados digitais na cédula profissional eletrónica da Ordem dos Médicos. [54]

A proposta começa com a desmaterialização dos contractos celebrados entre o profissional de saúde e as empresas de software de PEM, com autenticação do médico via internet, usando a CPE. Depois de confirmada a identidade e a autorização de prescrição, é gerada uma senha descartável (*one-time pad*), enviada para o contacto do médico registado nos SPMS (via telemóvel, correio eletrónico ou correio normal). Após a introdução da senha recepcionada, o médico fica associado à empresa e a SPMS seria notificada dessa contratação. A funcionalidade de consulta do histórico de

prescrições realizadas passaria a ser realizada através da PDS, igualmente após a autenticação do prescritor com recurso à CPE.

A integração do profissional prescritor no SPE proposto começa com a inscrição na plataforma da SPMS, apenas possível após autenticação com o CPE. Depois de validada a identidade e a situação atual do profissional (isto é, se está autorizado a exercer) é criado um canal seguro de transmissão de dados para a inscrição na SPMS. A inscrição implica a introdução dos dados de identificação do prescritor (ou importação dos mesmos a partir dos registos da Ordem dos Médicos) com discriminação dos estabelecimentos onde exerce funções (lista obtida a partir dos registos da ERS). Este processo é finalizado com a atribuição de uma senha aleatória de 256 bits, que seria cifrada com a chave pública do prescritor efectuada nos servidores da SMPS, transmitida para o terminal do médico e gravada apenas com permissões de leitura no cartão profissional (Figura 32).

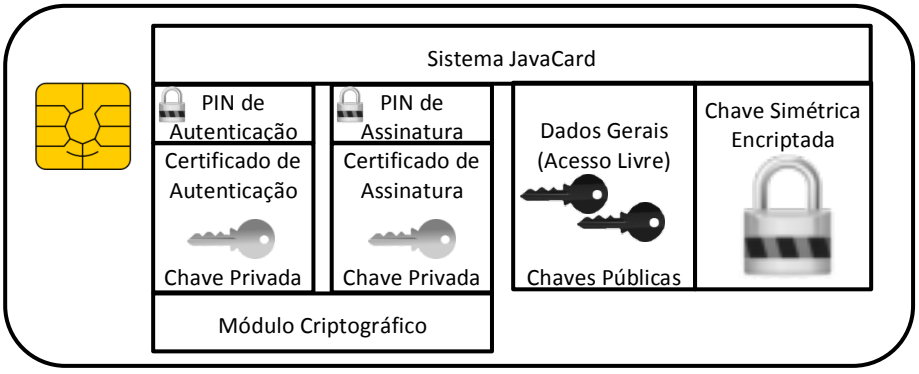


Figura 32: Modelo do Cartão Profissional Eletrónico proposto

Desta forma, a chave simétrica cifrada apenas poderá ser usada após a introdução código PIN, que protege o certificado e a decifra da mesma com a chave privada, impedindo o próprio médico de ter conhecimento da chave que lhe foi atribuída (Figura 33).

Este método permitira cifrar de forma eficiente usando criptografia simétrica, em que a chave apenas está registada em 2 locais: o CPE do médico e o servidor dos SPMS.

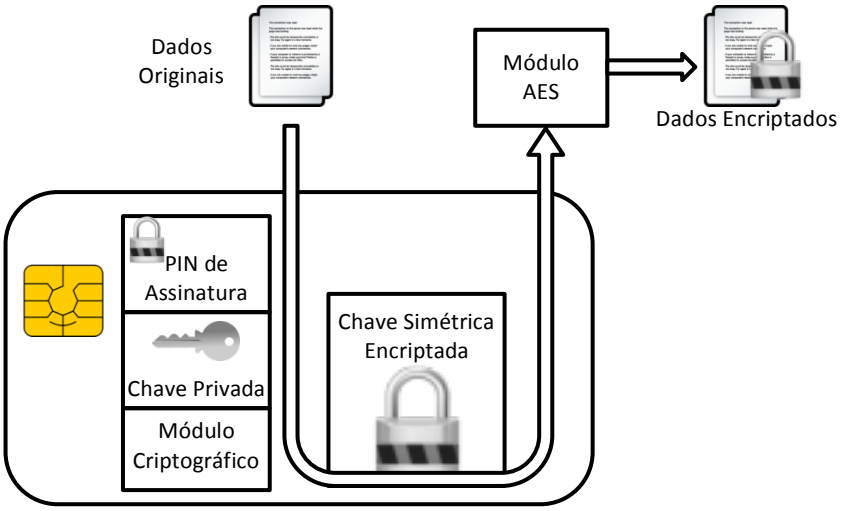


Figura 33: Encriptação de documentos a partir da chave simétrica do CPE

Com estes mecanismos é possível cifrar (recorrendo à chave simétrica) e autenticar (recorrendo à assinatura digital) os dados das prescrições. Estes são cifrados pela chave simétrica atribuída pela SPMS, que por sua vez ficam encapsulados pela chave privada do médico, sob a forma de uma assinatura digital com carimbo temporal (Figura 34).

Os vários softwares de PEM devem ainda ser dotados de um mecanismo de autenticação através do CPE, com acesso à chave privada de autenticação (protegida pelo PIN correspondente). Este mecanismo de acesso é facilmente implementável nos meios hospitalares, cuidados de saúde primários e restantes estabelecimentos de saúde permitindo também solucionar a problemática de partilha de credenciais de acesso e de abandono dos terminais informáticos com sessão aberta. Ao remover o

cartão, a sessão é suspensa, com gravação dos dados introduzidos se não houver uma reautenticação nos minutos seguintes.

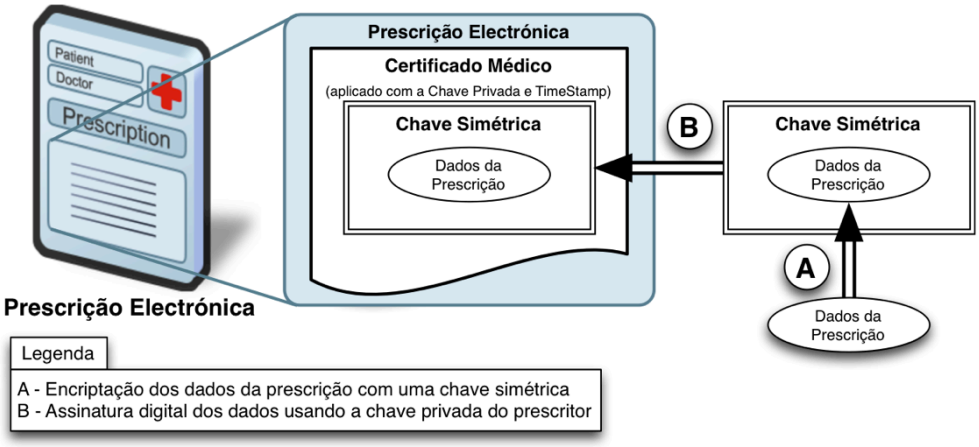


Figura 34: Proteção proposta dos dados das PEM

Durante o ato de prescrição, o médico pode selecionar a lista de medicamentos pretendidos, dosagem e posologia. Ao finalizar, é pedido o código PIN de assinatura que deve ser introduzido durante cada ato de prescrição. Depois de desbloqueado o acesso ao módulo que contém a chave privada de assinatura, o conteúdo da prescrição é cifrado e sobre este é calculado um resumo (*hash*), ao qual é aplicada a assinatura digital do médico.

A vantagem deste formato consiste em permitir às empresas de *software* e a SPMS verificar a autenticidade da informação recebida (com o uso da chave pública do médico) e somente a SPMS podem ter acesso ao conteúdo da informação, uma vez que a chave é apenas partilhada entre eles, como se esquematizou na Figura 35. Deste modo, as empresas de

software de PEM podem continuar a promover e assistir a prescrição eletrónica com confidencialidade dos dados dos utentes.

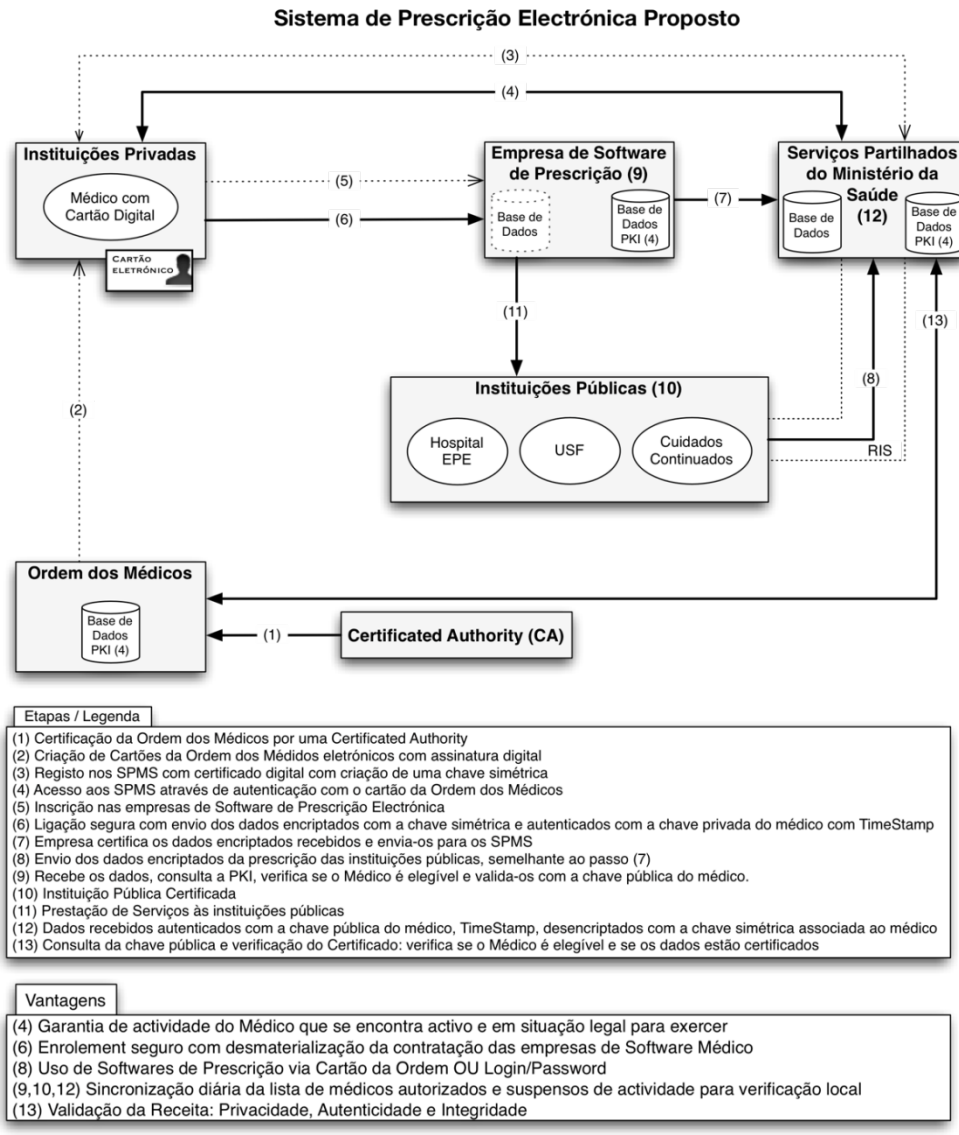

Sistema de Prescrição Electrónica Proposto
(3)
(4)
Instituições Privadas
Médico com Cartão Digital
CARTÃO ELETRÓNICO
(5)
(6)
Empresa de Software de Prescrição (9)
Base de Dados
Base de Dados PKI (4)
(7)
Serviços Partilhados do Ministério da Saúde (12)
Base de Dados
Base de Dados PKI (4)
(11)
(13)
(8)
(2)
Instituições Públicas (10)
Hospital EPE
USF
Cuidados Continuados
RIS
Ordem dos Médicos
Base de Dados PKI (4)
(1)
Certificated Authority (CA)
Etapas / Legenda
(1) Certificação da Ordem dos Médicos por uma Certificated Authority
(2) Criação de Cartões da Ordem dos Médidos eletrónicos com assinatura digital
(3) Registo nos SPMS com certificado digital com criação de uma chave simétrica
(4) Acesso aos SPMS através de autenticação com o cartão da Ordem dos Médicos
(5) Inscrição nas empresas de Software de Prescrição Electrónica
(6) Ligação segura com envio dos dados encriptados com a chave simétrica e autenticados com a chave privada do médico com TimeStamp
(7) Empresa certifica os dados encriptados recebidos e envia-os para os SPMS
(8) Envio dos dados encriptados da prescrição das instituições públicas, semelhante ao passo (7)
(9) Recebe os dados, consulta a PKI, verifica se o Médico é elegível e valida-os com a chave pública do médico.
(10) Instituição Pública Certificada
(11) Prestação de Serviços às instituições públicas
(12) Dados recebidos autenticados com a chave pública do médico, TimeStamp, desencriptados com a chave simétrica associada ao médico
(13) Consulta da chave pública e verificação do Certificado: verifica se o Médico é elegível e se os dados estão certificados
Vantagens
(4) Garantia de actividade do Médico que se encontra activo e em situação legal para exercer
(6) Enrolement seguro com desmaterialização da contratação das empresas de Software Médico
(8) Uso de Softwares de Prescrição via Cartão da Ordem OU Login/Password
(9,10,12) Sincronização diária da lista de médicos autorizados e suspensos de actividade para verificação local
(13) Validação da Receita: Privacidade, Autenticidade e Integridade

Figura 35: Esquema do Sistema Proposto de Prescrição Eletrónica

Uma das desvantagens deste método prende-se com a impossibilidade de realizar prescrições unicamente com recurso a plataformas web, sendo necessário a inclusão de um módulo local (sob a forma de software ou middleware) que realize a cifra dos dados com a assinatura do CPE.

Com esta proposta garante-se que:

- é validada a atividade dos médicos legalmente autorizados a prescrever;
- se realiza um auto-registo (*enrolement*) seguro com desmaterialização da contratação das empresas de software médico;
- o acesso aos softwares de prescrição via Cartão da Ordem dos Médicos;
- atualizar rapidamente a lista de profissionais com licença para atividade autorizada ou revogada;
- validar as prescrições mantendo a integridade dos dados;
- manter a privacidade e confidencialidade dos dados do utente.

6 SPE Proposto - Modelo físico

O modelo físico da prescrição eletrónica tem coexistido desde o início da implementação dos vários SPE, com a impressão dos medicamentos, doses e posologias numa folha A4, juntamente com a identificação do médico, instituição de saúde, regimes de comparticipação e número da receita (Figura 27, página 81).

Com a aposta num processo de dispensa eletrónica, o modelo de Prescrição Manual tenderá a ser usado menos frequentemente. No entanto, pode corresponder a uma solução para permitir a prescrição em situações de falhas do sistema ou das redes de comunicação. Neste sentido, optou-se por uma proposta de prescrição materializada em que é entregue ao utente um documento impresso equivalente à informação enviada digitalmente para a SPMS, que garanta o anonimato e a privacidade dos dados pessoais dos utentes.

As atuais receitas impressas apresentam duas áreas destacáveis entre si: a área da Prescrição (com os todos os dados clínicos, entregue ao farmacêutico) e a área da Guia de tratamento (que fica na posse do utente). Nesta proposta, mantém-se a secção da Guia de tratamento onde consta a identificação do utente, o nome do médico prescritor, a instituição a que este pertence, e os medicamentos prescritos com as respectivas posologias, comparticipações e preços. A primeira parte da receita, pretende-se que apresente um formato diferente, composto pelo logótipo e por dois códigos

em matriz (*QR-Code*) que representam a prescrição em si e um mecanismo de segurança para ser usado em caso de falha do sistema (Figura 36). A secção referente à descrição dos medicamentos mantinha-se como a original, de forma a permitir uma leitura humana rápida da medicação codificada ou descrever medicamentos sem CNPEM. O número da receita manter-se-ia em numeração arábica para possível introdução manual da receita, caso qualquer dos sistemas previstos falhem. As secções seguintes pretendem descrever pormenorizadamente a elaboração da cada um dos QR-Codes.

Este posicionamento estratégico dos QR-Codes no quadrante superior esquerdo, previne a deterioração dos mesmos quando os utentes dobram a receita em 2 ou em 4 partes, ficando o QR-Code da Prescrição ligeiramente afastado da divisão central da folha impressa.

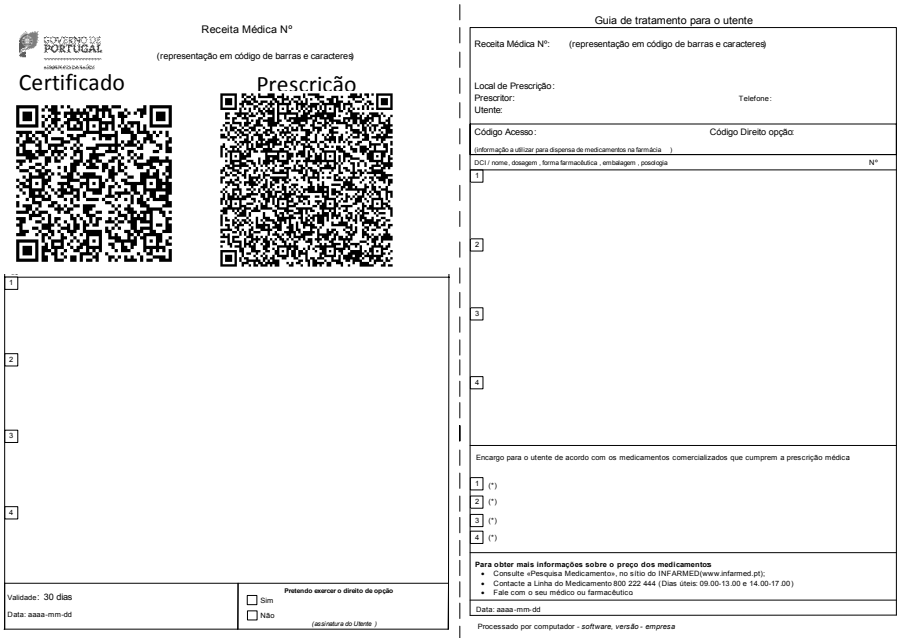

Receita Médica Nº
(representação em código de barras e caracteres)
Certificado
Prescrição
1
2
3
4
Validade: 30 dias
Data: aaaa-mm-dd
Pretendo exercer o direito de opção
Sim
Não
(assinatura do Utente)
Guia de tratamento para o utente
Receita Médica Nº: (representação em código de barras e caracteres)
Local de Prescrição:
Prescritor:
Telefone:
Utente:
Código Acesso:
Código Direito opção:
(informação a utilizar para dispensa de medicamentos na farmácia)
DCI / nome, dosagem , forma farmacêutica , embalagem , posologia
Nº
Encargo para o utente de acordo com os medicamentos comercializados que cumprem a prescrição médica
(*)
Para obter mais informações sobre o preço dos medicamentos
Consulte «Pesquisa Medicamento», no sítio do INFARMED(www.infarmed.pt);
Contacte a Linha do Medicamento 800 222 444 (Dias úteis: 09.00-13.00 e 14.00-17.00)
Fale com o seu médico ou farmacêutico
Data: aaaa-mm-dd
Processado por computador - software, versão - empresa

Figura 36: Modelo proposto da PEM impressa em papel

Quanto às dimensões, assumindo que a captura dos dados será feita a cerca de 15-20 cm, é essencial que este tenha um tamanho mínimo de 30mm (Figura 37).

Figura 37: Exemplo de um QR-Presc e QR-Cert com 35 mm de lado

6.1 QR-Code da Receita (QR-Presc)

Analisando os dados exigidos pela SPMS durante o registo de uma prescrição eletrónica [88], foi elaborada uma tabela para contabilizar as dimensões de cada campo (Tabela V).

Tabela V: Campos necessários para o processo de dispensa de uma PEM

	Campo	Bytes
	Número de Ordem do Médico	5
Assinados digitalmente	Número de Utente	9
	Número da Receita	13
	Data da Receita	8
	Validade (dias)	3
	Sistema de Saúde do utente	2
	Receita – Renovável	1
	Receita – Vias	1
	Medicamento – CNPEM	8 x 4
	Medicamento – Medicação Especial	1 x 4
	Medicamento – Nº Embalagens	1 x 4
	Medicamento – Comparticipação	3 x 4
	Medicamento – Troca por Genéricos	1 x 4
	Total	98

No momento da dispensa das receitas, apenas consta um número reduzido de informações que são realmente indispensáveis para as farmácias.

O número da ordem, no início do código vai servir como identificador da chave pública a ser requerida que permitirá a descodificação da restante informação contida no QR-Presc (Tabela V). O resto dos dados ficam assinados digitalmente pelo médico: o número da receita (13 algarismos), a data (8 dígitos) e a validade da mesma (3 dígitos), o sistema de saúde que se aplica (código de 2 dígitos), se a receita é renovável (e caso o seja, o número de vias da receita). No mesmo código estão incluídas as informações dos medicamentos (quatro no máximo, como mandam as

regras de prescrição atuais [10]): o Código Nacional para a Prescrição Eletrónica de Medicamentos (CNPEM), o número de embalagens prescritas, a comparticipação do medicamento em forma de valor percentual, e o campo de autorização de troca por genérico que codifica a justificação técnica do prescritor quanto à possibilidade de substituição do medicamento prescrito por um genérico.

Foram recentemente publicadas, pelo Infarmed (Autoridade Nacional do Medicamento e Produtos de Saúde IP), normas que regulamentam a identificação dos medicamentos prescritos através do CNPEM. [89, 90] O CNPEM agrupa a substância ativa (designada pela Denominação Comum Internacional - DCI), pela forma farmacêutica, dosagem e apresentações equivalentes, bem como critérios complementares de identificação, para efeitos de prescrição, dispensa e conferência de medicamentos. Esta codificação é realizada com 7 dígitos acrescidos de um dígito de controlo.

Caso exista um medicamento sem atribuição de um CNPEM, este fica apenas discriminado em forma de campo de texto no inferior da secção da prescrição.

Ao combinar as várias informações da prescrição numa só cadeia de dados, é possível gerar um código em matriz da mesma (*QR-Codes - Quick Response Codes*). Estes têm capacidade de armazenar mais informação que os tradicionais códigos de barras (Tabela VI) e possuem um mecanismo corretor de erros, que permite a recuperação de até 30% de dados perdidos em caso de dificuldades de leitura ótica.

Uma vez que os *QR-Codes* têm capacidade para armazenar mais de quatro quilobytes de caracteres alfanuméricos [91] (Tabela VI), a utilização dos mesmos com menos de 200 caracteres de tamanho é perfeitamente

aplicável, sendo lidos não só por dispositivos laser, mas também por outros dispositivos dotados de uma câmara.

Tabela VI: Capacidade máxima de dados de QR-Codes

Dados	Capacidade Máxima	Caracteres
Numérica	7,089 caracteres	0123456789
Alfanumérica	4,296 caracteres	0–9, A–Z [Só letras Maiúsculas], espaço, $, %, *, +, -, ., /, :
Binário	2,953 caracteres	8-bit bytes

Fonte: QRCode.com [91]

A geração dos dados da prescrição sob a forma de QR-Code foram batizados de "QR-Presc". Com o QR-Presc é possível garantir a privacidade dos dados pessoais do utente, que apenas tem de apresentar um comprovativo (cifrado) de que é credor dos medicamentos e benefícios descriminados na receita.

Para experimentar a conversão, foi criado um certificado de 1024 bits e, com o auxílio da ferramenta Cryptool 2* e QREncoder† foram estudadas as melhores opções (uso de dados binários e compressão gzip) para a criação dos QR-Codes com as menores dimensões possíveis.

Optou-se por aplicar uma assinatura digital à mensagem inicial e convertê-la para Base64, de forma a transformar o texto binário em caracteres facilmente legíveis para qualquer dispositivo (letras, números e símbolos matemáticos básicos).

* Cryptool 2 - http://www.cryptool.org/en/cryptool2

† QREncoder - www.mobiliodevelopment.com/qrencoder

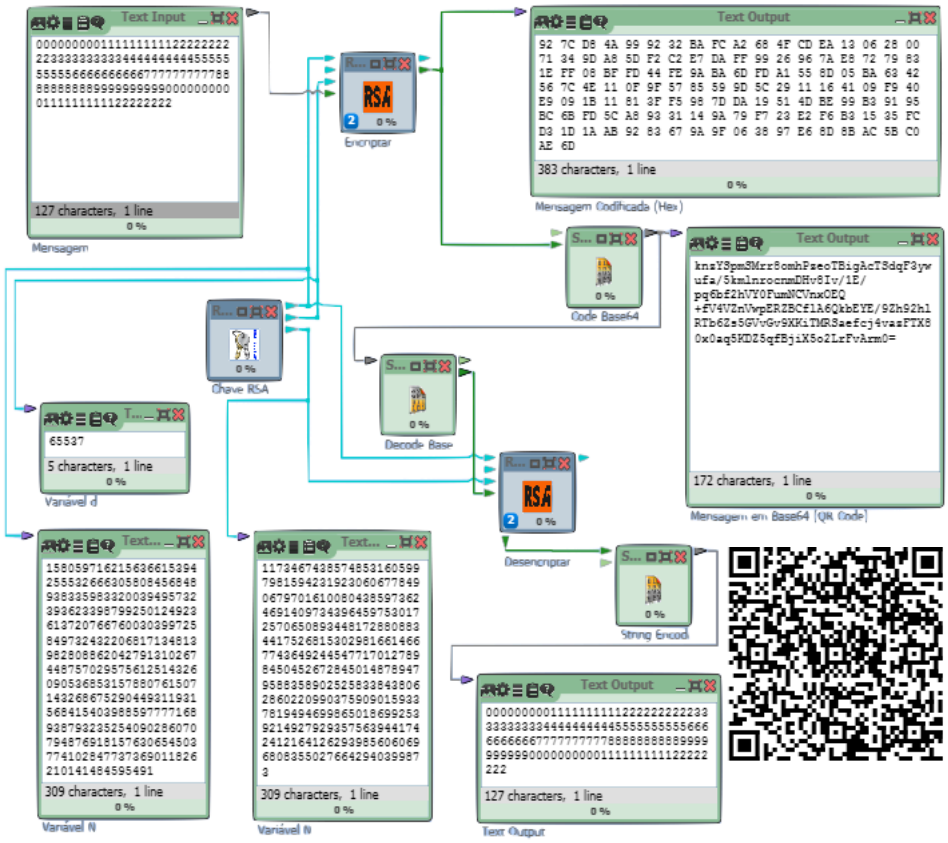


Figura 38: Computação da receita em QR-Code (Cryptool 2.0)

Neste modelo, verificou-se que com o processamento de mensagens com dimensões inferiores a 128 caracteres, a assinatura se mantém fixa em 383 códigos hexadecimais. Aplicada uma conversão para Base64, obtemos uma sequência de 172 caracteres, aos quais se acrescentam os 5 dígitos do número da ordem que depois são processados numa matriz de dados, como se esquematiza na Figura 38.

No momento da dispensa, o farmacêutico, com uma simples leitura do QR-Presc da Receita, tem acesso a todas as informações necessárias para

dispensar o medicamento, sendo a informação enviada para os SPMS e o CCF que em tempo real devolvem a veracidade da receita (sem ser necessário a identificação do utente) e a comparticipação de cada medicamento dispensado (Figura 39).

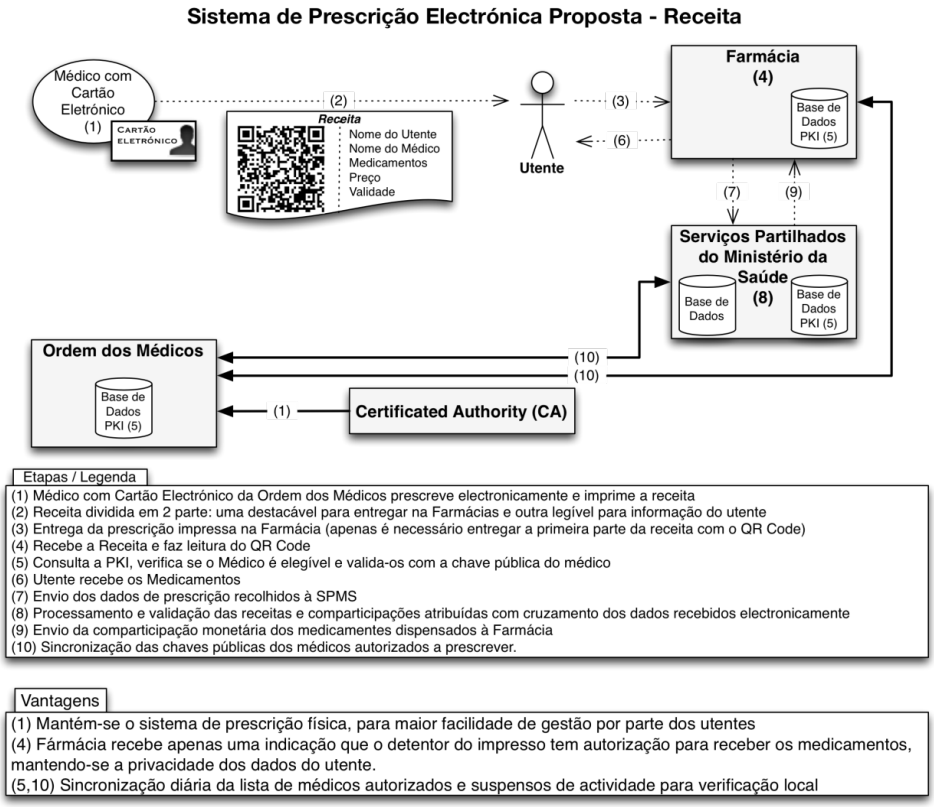

Sistema de Prescrição Electrónica Proposta - Receita
Médico com Cartão Eletrónico
(1)
CARTÃO ELETRÓNICO
(2)
Receita
Nome do Utente
Nome do Médico
Medicamentos
Preço
Validade
Utente
(3)
(6)
Farmácia
(4)
Base de Dados PKI (5)
(7)
(9)
Serviços Partilhados do Ministério da Saúde
(8)
Base de Dados
Base de Dados PKI (5)
Ordem dos Médicos
Base de Dados PKI (5)
(10)
(10)
(1)
Certificated Authority (CA)
Etapas / Legenda
(1) Médico com Cartão Electrónico da Ordem dos Médicos prescreve electronicamente e imprime a receita
(2) Receita dividida em 2 parte: uma destacável para entregar na Farmácias e outra legível para informação do utente
(3) Entrega da prescrição impressa na Farmácia (apenas é necessário entregar a primeira parte da receita com o QR Code)
(4) Recebe a Receita e faz leitura do QR Code
(5) Consulta a PKI, verifica se o Médico é elegível e valida-os com a chave pública do médico
(6) Utente recebe os Medicamentos
(7) Envio dos dados de prescrição recolhidos à SPMS
(8) Processamento e validação das receitas e comparticipações atribuídas com cruzamento dos dados recebidos electronicamente
(9) Envio da comparticipação monetária dos medicamentes dispensados à Farmácia
(10) Sincronização das chaves públicas dos médicos autorizados a prescrever.
Vantagens
(1) Mantém-se o sistema de prescrição física, para maior facilidade de gestão por parte dos utentes
(4) Fármácia recebe apenas uma indicação que o detentor do impresso tem autorização para receber os medicamentos, mantendo-se a privacidade dos dados do utente.
(5,10) Sincronização diária da lista de médicos autorizados e suspensos de actividade para verificação local

Figura 39: Sistema Proposto para o modelo físico da Prescrição Eletrónica

Este modelo, complementa a proposta da secção anterior, na medida em que, não só incrementa os níveis de segurança e de privacidade dos dados do utente como se traduz numa poupança de tempo de leitura da receita (que no modelo anterior implica a leitura de múltiplos códigos de barras), quer na farmácia, quer no CCF.

6.2 QR-Code do Certificado (QR-Cert)

Como explicado inicialmente, as receitas impressas incluem duas áreas de dados em matriz. A primeira corresponde ao QR-Presc, descrito anteriormente e a segunda serviria apenas para autenticar a prescrição em casos de inoperacionalidade dos sistemas de comunicação com os SPMS e o CCF.

A certificação da prescrição impressa, pode ser facilmente realizada com a leitura de um "mini-certificado" em forma de QR-Code, ao que denominamos "*QR-Cert*". O objectivo deste formato consiste em subtrair as informações adicionais dos certificados, resumindo-os a alguns identificadores básicos e à chave pública do médico. Sobre esta informação é aplicada uma chave privada de uma entidade nacional que deverá ser a Ordem dos Médicos. Desta forma é possível autenticar a receita com uma assinatura do médico, por sua vez, certificada pela Ordem dos Médicos.

A operacionalidade deste modelo tem como pré-requisito a instalação nos vários terminais das farmácias o certificado público da Ordem dos Médicos. Uma vez que o conteúdo do QR-Cert é estático quanto o certificado do médico, este apenas precisa de ser gerado uma vez, ficando associado ao certificado do médico (e possivelmente armazenado no CPE).

Este método tem a vantagem de, sem recorrer aos repositórios dos certificados médicos, poder certificar a assinatura pública do médico prescritor e a prescrição realizada pelo mesmo.

O QR-Cert é constituído por campos de identificação do médico, código da especialidade (para validar a prescrição de medicamentos restritos a determinadas especialidades), o formato e a versão do certificado e a chave

pública do médico (que autentica a prescrição entregue ao farmacêutico). Sobre estas informações é aplicado um hash com recurso ao algoritmo MD5 (Message-Digest Algorithm) que por sua vez é assinado digitalmente pela ordem dos médicos. A assinatura desta "impressão digital" tem um tamanho de 172 bytes, pelo que o código final totaliza 311 bytes, como se verifica na Tabela VII.

Tabela VII: Campos do QR-Cert

Campo	Bytes
Número de Ordem	5
Especialidade	2
Versão	2
Formato	2
Chave pública do Médico	128
Assinatura da Ordem dos Médicos	172
Total	311

Uma forma tornar este processo mais fácil de aplicar seria reduzindo as dimensões da assinatura da ordem. Uma forma de o realizar é com o uso de chaves de curvas elípticas que permitem obter certificados de menores dimensões. O algoritmo desta classe mais conhecido é o DSA (Digital Signature Algorithm) que serve de base às assinaturas DDS (Digital Signature Standard) [92] A grande diferença entre os algoritmos DSA e RSA pode ser resumido ao tamanho da assinatura e o tempo de validação da mesma: o DSA exige maior poder computacional mas gera assinaturas de menores dimensões. [93] Desta forma, uma chave usando o algoritmo DSA de 80 bytes é equivalente, em termos de segurança, a uma chave gerada pelo algoritmo RSA de 128 bytes. [94]

Supondo um cenário hipotético onde as farmácias se encontram impedidas de comunicar com os servidores da SPMS e os repositórios médicos, a existência do QR-Cert permite validar a receita recepcionada.

Dado que todas as farmácias teriam o certificado público da ordem instalado localmente, podemos assumir, com toda a segurança, que o hash do certificado do médico guardado no QR-Cert é autêntico. Da mesma forma, podemos tirar essa conclusão dos dados de prescrição, se esta for corretamente validada pelo certificado do médico. Quando o sistema retoma, o farmacêutico apenas tem que enviar os registos pendentes, com verificação dos números de receita validados e marcação dos mesmos como dispensados.

Por definição, a identidade do utente mantém-se anónima perante o farmacêutico, a menos que este deseje ser identificado, por motivos pessoais ou monetários. O exemplo típico é a emissão de factura para apresentar num subsistema de saúde. Dados os avanços tecnológicos nos registos e faturação eletrónica, as despesas de saúde são automaticamente associadas ao utente para posterior declaração nas entidades fiscais estatais.

À semelhança com qualquer sistema de autenticação sem comunicação com a rede, não é possível excluir a hipótese de múltiplas dispensas da mesma prescrição, motivo pelo qual se mantém a assinatura médica como forma de legitimar a prescrição.

Com esta proposta garante-se que:

- Se realiza um processo de certificação em tempo real da prescrição, quer por via eletrónica, quer por leitura ótica, das receitas impressas;
- Se otimiza o processo de dispensa nas farmácias (com a leitura de um único conjunto de dados);
- Se mantém a privacidade dos dados do utente com omissão da identidade do mesmo, a menos que o próprio não o deseje;
- Caso o haja falha dos sistemas, seja possível autenticar a prescrição com base nos certificados públicos do médico e da Ordem dos Médicos.

7 Conclusões

Na área da saúde lida-se com imensas informações pessoais e clínicas dos profissionais de saúde e dos pacientes. Estes dados podem com facilidade ser convertidos em valores económicos capazes de afetar não só os próprios indivíduos envolvidos como os seus familiares (em caso de alterações genéticas) durante várias gerações.

No inquérito realizado verificou-se que os médicos portugueses não se encontram conscientes de todos os riscos existentes no atual sistema de prescrição eletrónica. É espectável que as respostas obtidas representem uma população de profissionais médicos com um maior nível de conhecimento relativo à segurança dos dados clínicos, por estes serem os responsáveis pelos sistemas de prescrição adquiridos. Por esse motivo, é possível que a amostra não seja representativa da realidade portuguesa e, como tal, os resultados nacionais sejam mais graves do que os obtidos.

Das conclusões do questionário é de salientar a necessidade de informar os vários intervenientes no processo da prescrição (prescritores e utentes) quanto aos deveres e direitos de cada um e à forma como a informação circula nas redes de informação, de forma a promover a transparência dos sistemas de saúde em Portugal. A CNPD terá um papel fundamental neste processo como agente regulador do cumprimento das regras relativas à proteção de dados clínicos e pessoais, por parte do ministério, das

empresas de software, das entidades de saúde e dos profissionais de saúde envolvidos.

O processo de prescrição eletrónica em Portugal, não se encontra completamente informatizado e recorre ainda à impressão das mesmas de forma a permitir a dispensa dos medicamentos. O objetivo final das remodelações verificadas e agendadas ao nível do sistema de saúde é a implementação de um verdadeiro SPE, com desmaterialização e transmissão eletrónica dos dados. Comparado com os sistemas de outros países, conclui-se que a implementação de um SPE se associa inevitavelmente a medidas de segurança e privacidade dos dados, que representam um dos pilares fundamentais qualquer SPE bem implementado.

Um dos objetivos principais deste trabalho consiste em chamar a atenção para as várias falhas existentes no sistema de prescrição eletrónica e para os aspectos de segurança e privacidade dos dados, que são reconhecidos a nível mundial como uma preocupação de relevo. No sistema de prescrição atualmente implementado foram várias as falhas detetadas, quer de segurança, quer privacidade.

A proteção dos dados clínicos trata-se de uma matéria de extrema importância, que pode ser traduzida em dados económicos, para o médico, o próprio paciente ou familiares do mesmo. Este impacto pode ainda ser propagado a gerações futuras, nomeadamente quando se lida com patologias de transmissão genética, contagiosas ou responsáveis por limitações funcionais.

Portugal assume neste momento uma evolução exponencial na área da prescrição eletrónica. Este crescimento é mais um motivo para se fortificar

o sistema atualmente em vigor para que este resista e evolua de forma saudável e com o mínimo de fraudes possíveis. Tendo em conta a preocupação demonstrada pelo Ministério da Saúde em atualizar o atual SPE, é essencial reforçar os aspetos focados ao longo deste trabalho, de forma robusta e capaz de sustentar as alterações propostas:

- as empresas de software de prescrição devem ser devidamente certificadas com auditorias periódicas de forma a garantir que o funcionamento de acordo com a legislação e as exigências em vigor;
- os contratos estabelecidos com os médicos que pretendem aderir ao SPE elaborados pelas empresas de software privadas precisam de ser reformulados de forma a garantir a privacidade e simultaneamente autenticidade dos profissionais, com recurso ao cartão profissional eletrónico;
- o acesso dos profissionais de saúde deve passar a ser feito de forma a limitar a partilha de credenciais de acesso, através do mesmo cartão profissional, de forma a limitar o acesso aos sistemas de prescrição e incentivar à não partilha das mesmas;
- os dados transmitidos desde a estação de trabalho do médico até aos servidores dos SPMS devem estar devidamente protegidos de forma a assegurar a autenticidade e o não repúdio dos atos médicos;
- a prescrição impressa, enquanto existir, deverá apenas conter as informações necessárias para certificar ao farmacêutico que o utente é o destinatário dos medicamentos propostos, mantendo o direito à privacidade do utente.

A implementação do CPE é uma mais valia para o sistema de saúde e deve ser usado todo o potencial do mesmo. O sistema de prescrição proposto serve para demonstrar que o atual sistema pode ser corrigido de

forma económica, mantendo as infra-estruturas existentes com a implementação de simples medidas de segurança.

Relativamente ao CPE, pretende-se que, numa fase inicial, este valide os médicos que se encontram legalmente autorizados a prescrever; que a longo prazo represente um meio de identificação associada a autorizações que poderão ser adicionadas ou revogadas. Os algoritmos criptográficos existentes são uma solução viável para os problemas de segurança apontados. A opção proposta pretende usufruir das vantagens que cada método oferece, desde a segurança dos algoritmos de criptografia assimétrica à rapidez de computação da criptografia simétrica. Este tipo de tecnologia permite não só a identificação dos médicos perante as entidades de saúde ou outras instituições relacionadas (nomeadamente as empresas de software de prescrição eletrónica, com desmaterialização da contratação das empresas de software médico) como acesso e certificação dos mesmos aos sistemas de informação na área da saúde.

O uso de certificados digitais permite ainda uma rápida atualização (com autorização ou revogação) das licenças médicas, das credenciais de acesso a diversas áreas com registo e não repúdio das ações realizadas. A acrescentar a estes aspetos, temos ainda a vantagem de garantir a integridade dos dados e simultaneamente a privacidade e confidencialidade dos dados dos médicos e seus utentes. Do ponto de vista do farmacêutico, representa também uma poupança de tempo de leitura da receita (quer na farmácia, quer no CCF) e, como o processo ocorre em tempo real, permite certificar as prescrições e evitar processos de fraude com falsificação de prescrições.

A proposta para a prescrição em papel é apresentada como uma transição do atual sistema de prescrição enquanto não é adotado um verdadeiro SPE. Como explicado anteriormente, é importante apostar na segurança, confidencialidade e privacidade dos dados. A forma mais fácil e económica de o realizar será com a adoção de um sistema de transmissão de certificados digitais em papel. Para esse feito, recorreu-se ao uso de QR-Codes capazes de conter quer as informações das prescrições medicamentosas, quer o certificado do próprio médico (QR-Presc e QR-Cert, respetivamente), dada a capacidade de armazenamento dos códigos matriz e a informação que é necessário transmitir.

O modelo em papel, teria uma função principal de informar o utente dos medicamentos prescritos e em simultâneo de providenciar ao farmacêutico a mensagem de que ao detentor do mesmo impresso está reservado o direito de requerer o medicamentos, sem abdicar da sua privacidade. Para reforçar a segurança, os dados do QR-Presc encontram-se assinados digitalmente pela QR-Cert (assinatura do médico) que, por sua vez é assinada digitalmente pelo certificado da ordem dos médico. Este sistema vem permitir a sustentação de todo o sistema em caso de quebra de transmissão eletrónica.

Em tom de conclusão, este trabalho serve para demonstrar que, com os atuais recursos disponíveis é possível a implementação de um sistema de prescrição mais seguro e capaz de assegurar a confidencialidade e privacidade dos dados clínicos e pessoais envolvidos.

8 Trabalho Futuro

Tendo como base o sistema de prescrição proposto, pretende-se a elaboração de um protótipo funcionante do sistema de prescrição em linguagem Java™, capaz de encriptar dos dados de prescrição, certificar com um sistema chave pública-chave privada, encapsular os dados associados a um código de autenticação, transformar dos dados processados em QRCode, validar e desencriptar os dados de prescrição.

9 Anexos

9.1 Anexo 1: Questionário de Avaliação da Percepção dos Riscos de Segurança nos Profissionais de Saúde

Este questionário destina-se a profissionais médicos que exerçam medicina numa instituição privada. Os dados dos questionários serão tratados de uma forma anónima e confidencial.

1. Formação base:
□ Medicina
□ Outra

2. As suas credenciais de acesso (password) são conhecidas apenas por si?
□ Sim.
□ Não.
□ Não sei.

3. Acha possível outra pessoa prescrever em seu nome?
□ Sim.
□ Não.
□ Não sei.

4. Considera que, para a celebração do contracto com a empresa de prescrição eletrónica, cedeu demasiada informação pessoal?
□ Sim.
□ Não.
□ Não sei.

5. Acha que a informação pessoal cedida, se comprometida, potencia a fraude usando a sua identidade digital?
□ Sim.
□ Não.
□ Não sei.

6. De quem é a responsabilidade de informar o paciente que os seus dados clínicos são transmitidos através da internet para uma localização remota?
□ Empresa de Software
□ Médico prescritor
□ Não é necessário informar o paciente

7. De quem é a responsabilidade do registo da base de dados de prescrições junto da CNPD (Comissão Nacional de Proteção de Dados)?
□ Da empresa de software de prescrição

□ Do responsável da clínica
□ Não é necessário o registo junto da CNPD

8. Confia em empresas privadas para guardar os dados de prescrição médica dos seus pacientes?
□ Sim
□ Não

9. Qual ou quais das seguintes opções considera serem desvantagens da prescrição eletrónica? (pode marcar várias opções)
□ Necessidade de uso de um software, por parte do médico
□ Possibilidade da ocorrência de erros durante a prescrição
□ Impossibilidade de prescrever em caso de quebra de energia
□ Impossibilidade de prescrever em caso de não existir acesso à Internet
□ Preocupações ao nível da segurança dos dados dos doentes
□ Desconforto dos pacientes perante o uso de novas tecnologias
□ Outra *
(*) Se Outra, qual? _____

10. Onde imagina que fiquem guardados os registos das suas prescrições?
□ No computador de serviço
□ No servidor do meu departamento / da minha clínica
□ No servidor do meu fornecedor de serviços de prescrição
□ Num servidor fora do país
□ Outro local *
(*) Se Outro local, qual? _____

11. Na possibilidade dos fornecedores de software acederem aos seus registos de prescrições, quantifique o perigo que considera existir para os seus utentes.
□ 1 - Irrelevante; □ 2; □ 3; □ 4 - Muito Perigoso

12. Quantifique o interesse destas entidades em aceder aos dados das prescrições eletrónicas:
1 - Sem Interesse; 2 - Pouco interesse; 3 - Algum interesse; 4 - Muito interesse
12.1. Companhias de Seguros: □ 1; □ 2; □ 3; □ 4
12.2. Empresas de desenvolvimento de software: □ 1; □ 2; □ 3; □ 4
12.3. Laboratórios Farmacêuticos: □ 1; □ 2; □ 3; □ 4
12.4. Empresas de Marketing: □ 1; □ 2; □ 3; □ 4
12.5. Qualquer empresa durante a contratação de funcionários: □ 1; □ 2; □ 3; □ 4

13. Relativamente aos dados da prescrição eletrónica, como quantificaria o impacto / risco da quebra de privacidade nas seguintes situações:
1 - nenhum impacto; 2 - pouco impacto; 3 - bastante impacto; 4 - muito impacto
13.1. Valor dos seguros vida / saúde: □ 1; □ 2; □ 3; □ 4
13.2. Empréstimos bancários: □ 1; □ 2; □ 3; □ 4
13.3. Discriminação social: □ 1; □ 2; □ 3; □ 4
13.4. Procura de emprego: □ 1; □ 2; □ 3; □ 4

14. Para completar o inquérito, gostávamos de saber alguns dados gerais:
14.1. Sexo: □ Masculino; □ Feminino
14.2. Idade: ___ anos
14.3. Habilitações académicas:
□ Licenciatura
□ Mestrado
□ Doutoramento

14.4. Localidade da Residência
□ Açores
□ Aveiro
□ Beja
□ Braga
□ Faro
□ Bragança
□ Castelo Branco
□ Coimbra
□ Évora
□ Faro
□ Guarda
□ Leiria
□ Lisboa
□ Madeira
□ Portalegre
□ Porto
□ Santarém
□ Setúbal
□ Viana do Castelo
□ Vila Real
□ Viseu
□ Fora de Portugal

Para terminar, carregue em Gravar. Obrigado pela sua colaboração.

10 Referências

[1] M. D. Greenberg, M. S. Ridgely, and D. S. Bell, “Electronic prescribing and HIPAA privacy regulation”, Inquiry, vol. 41, pp. 461-8, Winter 2004.

[2] Diário da República, I Série-B, Nº287, Portaria n.º 1501/2002 (12 de Dezembro de 2002).

[3] Diário da República, I Série-A, Nº181, Decreto-Lei n.º 209/94 (6 de Agosto de 1994).

[4] Observatório Português do Sistema de Saúde, “Conhecer os caminhos da saúde: Relatório de primavera do OPSS”, 2001. - http://www.observaport.org/sites/observaport.org/files/RelatorioPrimavera2001_OPSS.pdf

[5] Diário da República, I Série, Nº195, Lei n.º 48/90 (24 de Agosto de 1990).

[6] Diário da República, I Série-A, Nº258, Lei n.º 27/2002 (8 de Novembro de 2002).

[7] Diário da República, 1ª Série, Nº56, Decreto-Lei n.º 19/2010 (22 de Março de 2010).

[8] Governo Português, “Memorando de Entendimento sobre as condicionalidades de Política Económica” (17 de Maio de 2011).

[9] Ministério das Finanças e da Administração Pública, “Programa de Estabilidade e Crescimento 2011-2014” (Março de 2011).

[10] Diário da República, 1ª Série, Nº96, Portaria n.º 198/2011 (18 de Maio de 2011).

[11] ACSS, “Manual de Relacionamento das Farmácias com o Centro de Conferência de Faturas do SNS “(Junho de 2012).

[12] Diário da República, 1ª Série, Nº38, Decreto-Lei n.º 28/2008 (22 de Fevereiro de 2008).

[13] Diário da República, 2ª Série, Nº126, Despacho n.º 8742/2012 (2 de Julho de 2012).

[14] Jornal Público, “Ordem vai criar um cartão mais seguro para médicos” (13 de Abril de 2012).

[15] Eurobarometer, Special edition 390 “Cyber Security Report”, 2012 (Julho de 2012).

[16] Infarmed, Circular Informativa Conjunta N.º 04/Infarmed/ACSS (20 de Dezembro de 2012).

[17] Jornal Correio da Manhã, “Cem suspeitos por fraudes na Saúde” (28 de Junho de 2012).

[18] Jornal de Negócios, “Fraude na saúde poderá atingir os 100 milhões de euros” (26 de Junho de 2012).

[19] Jornal Crime, “Dados privados de doentes à solta na internet” (27 de Setembro de 2012).

[20] ACSS, “Modelo de Declaração de Conformidade do Fabricante”, 2012.

[21] CNPD, Parecer n.º 16/2012 da CNPD, “Projecto de Portaria de regulamentação da Lei nº 11/2012” (8 de Março de 2012).

[22] ACSS, “Declaração de Confidencialidade para certificação de Software de Prescrição Electrónica - IMP009, v2”, 2011 (31 de Agosto de 2011).

[23] CNPD, “Relatório de Actividades da CNPD (2010)”, 2010.

[24] R. C. Barrows, Jr. Clayton, P. D., “Privacy, confidentiality, and electronic medical records”, J Am Med Inform Assoc, vol. 3, pp. 139-48, Mar-Apr 1996.

[25] K. D. Mandl, P. Szolovits, and I. S. Kohane, “Public standards and patients' control: how to keep electronic medical records accessible but private”, BMJ, vol. 322, pp. 283-7, Feb 3 2001.

[26] Diário da República, I Série-A, Nº247, Lei n.º 67/98, “Lei da Protecção de Dados Pessoais” (26 de Outubro de 1998).

[27] Estonia Health Insurance Fund, “Digital Prescription”. - http://www.haigekassa.ee/eng/digital_prescription

[28] T. K. et al., “Factorization of a 768-bit RSA modulus. Cryptology - ePrint Archive, 2010. 4”, 2010.

[29] S. Harris, CISSP Boxed Set: McGraw-Hill Education, 2011.

[30] W. Tuchman, “A brief history of the data encryption standard”, Internet besieged: countering cyberspace scofflaws. ACM Press/Addison-Wesley Publishing Co., pp. 275–280, 1997.

[31] NIST, “Federal Information Processing Standards Publications - Announcing the Advanced Encryption Standard (AES)”, 2001 (26 de Novembro de 2001).

[32] J. Nechvatal, et al, “Report on the Development of the Advanced Encryption Standard (AES)”, National Institute of Standards and Technology, 2/10/2000 2000.

[33] S. A. Rivest RL, Adleman L., “A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM” Fev;21(2):120-6, 1978.

[34] Diário da República, I Série-A, Nº79, Decreto-Lei n.º 62/2003 (3 de Abril de 2003).

[35] C. D. H. E., “Group signatures”, presented at the Proceedings of the 10th annual international conference on Theory and application of cryptographic techniques, Brighton, UK, 1991.

[36] G. Ateniese and G. Tsudik, “Some Open Issues and New Directions in Group Signatures”, presented at the Proceedings of the Third International Conference on Financial Cryptography, 1999.

[37] Y. Yang, X. Han, F. Bao, and R. H. Deng, “A smart-card-enabled privacy preserving E-prescription system”, IEEE Trans Inf Technol Biomed, vol. 8, pp. 47-58, Mar 2004.

[38] K. H. Lee B, Kim K., “Strong proxy signature and its applications. In: SCIS2001, vol. 2/2; January 23-26, 2001. p. 603-8”, 2001.

[39] S. A. Toorani M, “LPKI - A Lightweight Public Key Infrastructure for the Mobile Environments”, Proceedings of the 11th IEEE International Conference on Communication Systems (IEEE ICCS'08), 162-166, 2008.

[40] M. M. e. al, “The Internet Engineering Task Force - Online Certificate Status Protocol”, 1999.

[41] Projecto Cartão de Cidadão, “Manual técnico do Middleware Cartão - Janeiro 2012 - Versão1.24.1”, 2012.

[42] Diário da República, I Série-A, Nº115, Decreto-Lei n.º 116A/2006 (6 de Junho de 2006).

[43] Diário da República, 1ª Série, Nº70, Decreto-Lei n.º 88/2009 (9 de Abril de 2009).

[44] Diário da República, 1ª Série, Nº147, Decreto-Lei n.º 161/2012 (31 de Julho de 2012).

[45] International Organization for Standardization, “ISO/IEC 7810. Identification cards”, 2003.

[46] International Organization for Standardization, “ISO/IEC 14443. Identification cards -- Contactless integrated circuit cards -- Proximity cards”, 2008.

[47] International Organization for Standardization, “ISO/IEC 7816. Identification cards -- Integrated circuit cards”, 2011.

[48] Projecto Cartão de Cidadão, “Especificações - Leitores base - 14 de Junho de 2007 - Versão1.0”, 2007.

[49] European Patent Office, US4105156 (A), 1978-08-08 “Identification system safeguarded against misuse”, 1978.

[50] Oracle, "Java card technology providing a secure and ubiquitous platform for smart cards - http://www.oracle.com/technetwork/java/javacard/documentation/datasheet-149940.pdf," 2012.

[51] Diário da República, 1ª Série, Nº25, Lei n.º 7/2007 (5 de Fevereiro de 2007).

[52] Projecto Cartão de Cidadão, “Declaração de Práticas de Certificação da EC do Cidadão, 28 de Junho de 2012, Versão 1.2”, 2012.

[53] Entidade de Certificação Electrónica do Estado, “Documento de declaração de práticas de certificação - Entidade Certificadora Electrónica Raiz, 20 de Julho de 2006, Versão 1.0”, 2006.

[54] Ordem dos Médicos, “Nova Cédula Profissional”, 2012. - http://www.cartaoordemdosmedicos.com/

[55] A. J. Stroetmann K., Stroetmann V., “eHealth Strategies Report - European countries on their journey towards national eHealth infrastructures, Final European progress report”, 2011.

[56] AMA, “Clinician’s Guide to e-prescribing”, 2011.

[57] J. Niinimaki, M. Savolainen, and J. J. Forsstrom, “Methodology for security development of an electronic prescription system”, Proc AMIA Symp, pp. 245-9, 1998.

[58] J. Niinimaki and J. Forsstrom, “Approaches for certification of electronic prescription software”, Int J Med Inform, vol. 47, pp. 175-82, Dec 1997.

[59] V. M. Brannigan and B. R. Beier, “Patient privacy in the era of medical computer networks: a new paradigm for a new technology”, Medinfo, vol. 8 Pt 1, pp. 640-3, 1995.

[60] V. H. Dijk L., Bell D., “Electronic prescribing in the United Kingdom and in the Netherlands - Agency for Healthcare Research and Quality - RAND Europe2011”, 2011.

[61] D. P. Mundy and D. W. Chadwick, “Security issues in the electronic transmission of prescriptions”, Med Inform Internet Med, vol. 28, pp. 253-77, Dec 2003.

[62] C. J. Wang, R. S. Marken, R. C. Meili, J. B. Straus, A. B. Landman, and D. S. Bell, “Functional characteristics of commercial ambulatory electronic prescribing systems: a field study”, J Am Med Inform Assoc, vol. 12, pp. 346-56, May-Jun 2005.

[63] T. C. Hsiao, Z. Y. Wu, Y. F. Chung, T. S. Chen, and G. B. Horng, “A secure integrated medical information system”, J Med Syst, vol. 36, pp. 3103-13, Oct 2012.

[64] P. Kierkegaard, “E-Prescription across Europe”, Health and Technology, pp. 1-15, 2012/12/01 2012.

[65] W. P. van de Ven and F. T. Schut, “Universal mandatory health insurance in the Netherlands: a model for the United States?”, Health Aff (Millwood), vol. 27, pp. 771-81, May-Jun 2008.

[66] M. Makinen, P. Rautava, J. Forsstrom, and M. Aarimaa, “Electronic prescriptions are slowly spreading in the European Union”, Telemed J E Health, vol. 17, pp. 217-22, Apr 2011.

[67] F. Sullivan, “E-Prescription in Europe: First Things Fast”, 2007 (30 de Julho de 2007).

[68] F. Sullivan, “Market Insight, Smart Cards for Healthcare in Europe”, (3 de Maio de 2012).

[69] K. M., “European E-Prescriptions Market will reach $500mn by 2017”, 2011. - http://www.companiesandmarkets.com/News/Healthcare-and-Medical/European-E-Prescriptions-Market-will-reach-500mn-by-2017/NI2232

[70] Medcom, “eHealth in Denmark—eHealth as a part of a coherent Danish health care system - Danish Ministry of Health”, 2012.

[71] L. Hellstrom, K. Waern, E. Montelius, B. Astrand, T. Rydberg, and G. Petersson, “Physicians' attitudes towards ePrescribing--evaluation of a Swedish full-scale implementation”, BMC Med Inform Decis Mak, vol. 9, p. 37, 2009.

[72] epSOS, “Country profile: Sweden”, 2012. - http://www.epsos.eu/home/project-members-beneficiaries/participating-countries/sweden.html

[73] epSOS, “Country profile: Netherlands”, 2012 - http://www.epsos.eu/home/project-members-beneficiaries/participating-countries/netherlands.html

[74] epSOS, “Final epSOS System Technical Specification, D3.3.2, version 1.4”, 2010 (28 de Abril de 2010).

[75] epSOS, “Country status outline and template specification, D1.4.2, version 1.00”, 2012 (2 de Fevereiro de 2012).

[76] CNPD, Parecer n.º 66/2011 da CNPD, “Pedido da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias sobre a Proposta de Lei n.º 23/XII”, 2011.

[77] Diário da República, 1ª Série, Nº92, Portaria n.º 137-A/2012, 11 de Maio de 2012).

[78] Diário da República, 2ª Série, Nº238, Despacho n.º 15700/2012, 10 de Dezembro de 2012).

[79] Diário da República, 1ª Série, Nº31, Portaria n.º 46/2012, 13 de Fevereiro de 2012).

[80] APMGF, Jornal Médico de Família, Nº81, Fev/2005.

[81] Diário da República, 1ª Série-A, Nº18, Lei n.º 12/2005 (26 de Janeiro de 2005).

[82] T. Porteous, C. Bond, R. Robertson, P. Hannaford, and E. Reiter, “Electronic transfer of prescription-related information: comparing views of patients, general practitioners, and pharmacists”, Br J Gen Pract, vol. 53, pp. 204-9, Mar 2003.

[83] J. W. Bowen, J. C. Klimczak, M. Ruiz, and M. Barnes, “Design of access control methods for protecting the confidentiality of patient information in networked systems”, Proc AMIA Annu Fall Symp, pp. 46-50, 1997.

[84] F. H. France and P. N. Gaunt, “The need for security - a clinical view”, Int J Biomed Comput, vol. 35 Suppl, pp. 189-94, Feb 1994.

[85] Roger France FH, Gaunt PN, “Control and use of health information: a doctor’s perspective”, Inf J Biomed Comput, 43 (1996) 19-25.

[86] I. McLean and C. M. Anderson, “The security of patient identifiable information in doctors' homes”, J Clin Forensic Med, vol. 11, pp. 198-201, Aug 2004.

[87] CNPD, “Relatório de Actividades da CNPD (2011)”, 2011.

[88] ACSS, “Especificação Técnica - Base de Dados Nacional de Prescrições Interface para recepção de receitas medicas, ET.ACSS 20:2011/REV 2”, (29 de Junho de 2011).

[89] Infarmed, “Normas técnicas relativas à prescrição de medicamentos e produtos de saúde”, 2012.

[90] Infarmed, Circular Normativa N.º 001/CD/8.1.6, “Código Nacional para a Prescrição Eletrónica de Medicamentos - CNPEM”, (19/03/2013).

[91] QR Code, “High Capacity Encoding of Data”, 2010. - http://www.qrcode.com/en/qrfeature.html

[92] Federal Information Processing Standards Publication, “Digital Signature Standard (DSS)”, FIPS PUB 186-3, 2009.

[93] H. P., “DSA with SHA-2 for DNSSEC, draft-hoffman-dnssec-dsa-sha2-00”, 06/07/2009.

[94] H. P. Orman H., “Network Working Group , Determining Strengths For Public Keys Used For Exchanging Symmetric Keys”, 04/2004.

Todas as referências com ligações válidas confirmadas no dia 11 de Fevereiro de 2013